

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		1/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

関係各部署 御中 To departments concerned	Confidential level	<div>PROTECTED</div> <div>関係者外秘</div>	原紙保管 Storage of original	M/Y /
			コピー保管 Storage of copy	M/Y /

共通脆弱性対策要求仕様書 Requirements Specification of Common Vulnerability Countermeasure	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 E/E Architecture Development Div. System network & architecture development dept 4G			
	No. SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a			
	承認 Approved	調査 Checked	作成 Created	2023/3/30
	平林	平井	玉樹 清川 安江	<div>Omission of signature (approved electronically)</div>

適用先 Target	サイバーセキュリティ管理策を織り込む ECU ECUs that cybersecurity controls are incorporated.
---------------	--

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、ボデーメーカー、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 E/E Architecture Development Div. System network & architecture development dept. Contact for security inquiries E-mail: epf-sec-sp@mega.tec.toyota.co.jp
--------------------	--

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		2/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

変更履歴 ^{Δ1}

記号	Version	日付	変更者	項目	変更内容
	1.0	2016/8/12	51F 澤田	全項目	初版発行
Δ1	1.1	2016/10/28	51F 澤田	3.2.2.2	評価要件(SPC-E-0001)の明確化、表に記載
↑	↑	↑	↑	3.2.3.2	評価要件(SCD-E-0002)の明確化、表に記載
↑	↑	↑	↑	1.6	関連文書一覧の記載形式を箇条書きから表（表 1.3、表 1.4）に変更
↑	↑	↑	↑	2.2	評価方法の名称を変更
↑	↑	↑	↑	全項目	その他の誤記修正
Δ2	1.2	2017/4/24	51F 澤田	3.2.1.1	対策要件(PRV-0001)の対応期限の明確化、車載部品非開封の特権機能を残置可能な場合の明確化
↑	↑	↑	↑	3.2.5.1	対策要件(CSP-0001)にパスワードをマイコン外付けメモリに格納する場合の対策を追加
↑	↑	↑	↑	3.2.5.1	対策要件(CSP-0002) に CSP をマイコン外付けメモリに格納する場合の対策を追加
↑	↑	↑	↑	3.3.1.1	対策要件(TAC-0001)の対応期限の明確化
↑	↑	↑	↑	全項目	その他の誤記修正
Δ3	1.3	2017/7/31	51F 澤田	1.6	関連文書一覧の要件書名称を変更（「CCP/XCP 要件書」を「CCP/XCP セキュリティ要件書」に変更）
↑	↑	↑	↑	3	脆弱性対策・脆弱性対策織込み確認の各要件の並び順を変更
↑	↑	↑	↑	3.1.2	L2, L3 ECU の乱数エントロピー要求値を乱数用途毎の値に変更
↑	↑	↑	↑	全項目	その他の誤記修正
Δ4	1.4	2018/2/28	51F 澤田	1.5	CSP（表 1.1）の明確化
↑	↑	↑	↑	2.1	車載部品非開封の特権機能の利用（表 2.1）の明確化
↑	↑	↑	↑	3	用語、適用セキュリティレベルの明確化、エビデンス記載内容に評価要件(ID)を追加、要件織込み確認判断基準及び評価確認判断基準の明文化
↑	↑	↑	↑	全項目	その他の誤記修正
Δ5	1.5	2018/11/14	51F 尾崎	表紙	特記を追記

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		3/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

↑	↑	↑	↑	1.6	本文中で引用していない関連文書を削除、仕様書番号を追記、表 1.4 に「本書における略称」を追記
↑	↑	↑	51F 澤田	1.8	チェックリストとエビデンスの提出方法を追記
↑	↑	↑	51F 尾崎	3.1.2.1.	真性乱数生成器の使用方法の注釈を追記、アルゴリズム予測不可能性要求値を乱数用途毎に変更
↑	↑	↑	↑	3.2.1.1.	通知の時期を追記、禁止条件について注釈を追記
↑	↑	↑	51F 澤田	3.2.3.1.	外部調達ソフトウェア及びレガシーソフトウェアについて、逸脱手続きは、MISRA Compliance に従うこと、セキュリティ上許容の判断基準は、各言語に対応したセキュアコーディングルールの説明に記載されている非準拠の懸念点が無いことを明確化。コーディング主管部署のシンボル符号を PQF に変更。
↑	↑	↑	51F 澤田	全項目	セキュリティレベル L4 を削除、エビデンスについて「提出が必要な」という記載を削除
↑	↑	↑	51F 尾崎	↑	その他の誤記修正、本文中の参考文献 URL を削除
Δ6	2.0	2020/6/23	46F 菅野	1.2.	概要の削除
↑	↑	↑	↑	↑	本書の位置づけと適用フェーズの図を追記
↑	↑	↑	↑	1.3.	略語・用語解説の修正
↑	↑	↑	↑	1.4.	関連文書の修正
↑	↑	↑	↑	2.1.	トヨタとサプライヤ間での CIAD の締結についての節を追記
↑	↑	↑	↑	3.	本書の対象と適用条件の章を追記
↑	↑	↑	↑	4.2.	脆弱性対策の評価概要から攻撃の入口検索テストに関する記述を削除
↑	↑	↑	↑	5.1.	エビデンスの作成期限についての要件事項を追記
↑	↑	↑	↑	5.2.1.	暗号アルゴリズムが準拠すべき規格を CRYPTREC から FIPS、SP800-140C, D に変更 鍵長に関する要件を追記

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		4/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

↑	↑	↑	↑	5.3.1.	対策要件(PRV-0002)のパスワード長を 128bit 以上に変更
↑	↑	↑	↑	↑	対策要件(PRV-0002)の C&R 認証で使用するアルゴリズム、及び乱数は ARG-0001, RND-0001, RND-0002 を満たすことに変更
↑	↑	↑	↑	5.3.3.	対策要件(SCD-0001, SCD-0002)の適用セキュリティレベルの変更
↑	↑	↑	↑	5.3.5.	対策要件(CSP-0005)の(セッションキーに限る)という記載を削除
↑	↑	↑	↑	5.3.6.	評価要件(IFD-0001-R, IFD-0004-R)の表記法を他の評価要件と揃えるよう修正
↑	↑	↑	↑	5.4.1.	対策要件(TAC-0001)の C&R 認証で使用するアルゴリズム、及び乱数は ARG-0001, RND-0001, RND-0002 を満たすことに変更
↑	↑	↑	↑	5.4.2.	評価要件(ANL-0001-R, ANL-0004-R)の表記法を他の評価要件と揃えるよう修正
↑	↑	↑	↑	5.4.3.	対策要件(TMP-0008)として Glitch 攻撃対策の要件を追記
↑	↑	↑	↑	↑	対策要件(TMP-0009)としてタイミング解析対策の要件を追記
↑	↑	↑	↑	↑	評価要件(TMP-0003-R, TMP-0004-R, TMP-0005-R)の表記法を他の評価要件と揃えるよう修正
↑	↑	↑	↑	6.	既製品に対するセキュリティ要件を追記
↑	↑	↑	↑	全項目	対策要件、評価要件への適用条件の追記
↑	↑	↑	↑	↑	その他の誤記修正
↑	↑	↑	↑	表紙	文書名を変更、特記修正
↑	↑	↑	↑	全項目	要件 ID を VULCMN_XXXXX の形式に置き換え
Δ7	2.1	2020/12/18	46F 菅野	5.3.3.	セキュアコーディングの適用条件を変更
↑	↑	↑	↑	5.3.5.	PSP の保護要件を追記
↑	↑	↑	↑	5.3.6.	OS/OSS の脆弱性探索要件を削除
↑	↑	↑	↑	全項目	セキュリティレベルを目標 AP に変更
↑	↑	↑	↑	↑	その他の誤記修正、記載改善(補足追加等)
Δ8	2.2	2021/4/29	46F 石川	5.4.3.	耐タンパ要件の対象を CSP として明記
↑	↑	↑	↑	1.3.	略語(PSP)の追加

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		5/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

↑	↑	↑	↑	3.1. 5.2.2.1. 5.3.6.1. 5.3.6.2.	セキュリティレベルから目標 AP への記載修正
↑	↑	↑	↑	全ページ	ヘッダの記載変更
↑	↑	↑	↑	5.4.3.1.	グリッチ攻撃およびタイミング解析の対策例を追記
↑	↑	↑	↑	全項目	その他の誤記修正
↑	↑	↑	↑	全ページ	英訳の追加
Δ9	2.3	2021/7/30	46F 石川	5.3.6	アクセス権管理の要件を追記
↑	↑	↑	46F 早川	5.3.1 5.4.1	文字列により設定されるパスワード要件の追加
↑	↑	↑	↑	5.2.1	CSP の利用に関する要件の追加
↑	↑	↑	↑	5.3.6	ログイン機能に関する要件の追加
↑	↑	↑	46F 清川	4.1.	特権機能に該当するポート上の IP サービスを明確化
↑	↑	↑	↑	5.3.1.1	残置を許可する特権機能の条件を明確化
Δ10	2.4	2021/8/31	46F 垣屋	5.3.6	ログイン機能に関するパスワード要件の追加
↑	↑	↑	↑	↑	アプリに関するパスワード要件の追加
↑	↑	↑	46F 玉樹	5.3.5.1	セキュリティ IP 搭載要件の目標 AP, 適用条件、要件の記載改善
↑	↑	↑	46F 石川 46F 早川	5.2.2	C&R 認証に用いる乱数のエントロピー要件を変更
↑	↑	↑	↑	5.3.1	非開封の特権機能における認証失敗時のペナルティ要件(VULCMN_00600)を 5.2.2 乱数要件(VULCMN_00200)に統合し、当要件は削除
↑	↑	↑	46F 石川	5.3.6	アクセス権管理の要件(VULCMN_03700)の適用対象を変更
Δ11	2.5	2021/9/23	46F 玉樹	3.1	目標 AP の定義について参照先を追記
↑	↑	↑	46F 垣屋	1.3	用語解説にアプリの定義を追加
Δ12	2.6	2021/10/19	46F 安江	3.3	要件一覧を追加
↑	↑	↑	46F 玉樹	4.3.4	VULCMN_01500 を削除
↑	↑	↑	↑	4.2.2	SP800-90 に関する要件の追加

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		6/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

↑	↑	↑	46F 早川	1.3 1.4	適用範囲、要件の記載の章構成変更と内容明確化
↑	↑	↑	46F 垣屋	1.5 1.6	略語・用語解説を変更
↑	↑	2021/11/05	46F 玉樹	4.3.1.1	残置を許可する特権機能の条件を明確化
↑	↑	↑	↑	1.2	図 1-1 を削除
↑	↑	↑	↑	全項目	エビデンス要求の削除
↑	↑	↑	↑	4.4.3.1 4.4.3.2	VULCMN_03100, VULCMN_52100 を削除
↑	↑	↑	46F 垣屋	1.6 4.3.1.1	「情報セキュリティ特権機能一覧」の内容を本書に反映し、上記文書を関連文書一覧から削除
↑	↑	↑	46F 玉樹	4.3.6	VULCMN_02400, VULCMN_51500 を削除
↑	↑	↑	↑	4.2.2.1	VULCMN_00200 で真性乱数生成器を使用する場合のクラス指定を追加
Δ13	2.7	2022/3/1	46F 玉樹	4.3.5.1	セッションキーの保護要件(VULCMN_02000)を CSP・PSP の格納要件(VULCMN_01702)に統合し、セッションキーの保護要件(VULCMN_02000)は削除
↑	↑	2022/3/17	↑	4.3.5.1 4.4.1.1	セキュリティ IP を HSM に変更
↑	↑	2022/4/29	↑	4.3.5.1	セキュアメモリ、汎用 CPU、汎用メモリの用語を明確化
↑	↑	↑	↑	↑	CSP・PSP の保護要件の記載改善
↑	↑	2022/5/12	46F 垣屋	4.2.2.1	英語版の編集上の誤記修正
↑	↑	2022/5/17	46F 玉樹	4.3.5.1	パスワードの保護要件(VULCMN_01600)の適用条件と要件の明確化
↑	↑	2022/6/16	↑	4.2.2.1	乱数生成器で使用する暗号アルゴリズムの明確化
↑	↑	2022/6/22	46F 石川	4.3.3.1	TSC7030G, TSC7047G の改訂に対応 (CERT-C、CERT-C++の適用を明記)
↑	↑	2022/6/24	46F 安江	4.2.2.1 4.3.1.1 4.3.2.1 4.3.4.1	英語版の補足、例、理由内の表現明確化 (VULCMN_00200, VULCMN_00800, VULCMN_01100, VULCMN_01400, VULCMN_02200, VULCMN_02503)

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		7/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

				4.3.6.1 4.4.1.1	
Δ14	2.7	2022/6/30	46F 玉樹	4.2.2.1	SP800-90A の予測不可能性の要件を削除
↑	↑	2022/8/11	↑	4.2.2.1	128bit 乱数列衝突の要件の修正
↑	↑	2022/10/25	↑	4.3.6.1	TCP/UDP ポートの要件(VULCMN_02100)の明確化
↑	↑	↑	↑	4.3.2.1	トヨタ指示仕様以外の機能に関する要件(VULCMN_01000)の明確化
↑	↑	↑	↑	表紙	フォーマット変更
↑	↑	↑	46F 清川	4.3.5.1	PSP の保護に関する要件の明確化(VULCMN_01701, VULCMN_01702)
Δ15	a01-08-a	2022/11/10	46F 玉樹	5.1	既製品に対する単体評価の要件(VULCMN_52300)を削除
↑	↑	↑	↑	2.1	CIAD を CIA に変更
↑	↑	2022/11/17	46F 安江	4.3.1.1	セキュリティ主管部署が許可している特権機能の追加(VULCMN_00400)
Δ16	a01-09-a	<u>2023/1/13</u>	<u>46F 玉樹</u>	<u>4.3.2.2</u>	<u>トヨタ指示仕様以外の機能に関する評価要件(VULCMN_50600)の明確化</u>
↑	↑	<u>2023/1/25</u>	↑	<u>1.6</u>	<u>関連文書の削除</u>
↑	↑	↑	↑	<u>3.3</u>	<u>表 3-5 の修正</u>
↑	↑	↑	↑	<u>3.1</u>	<u>IP サービスの説明追記</u>
↑	↑	2023/2/14	46F 清川	4.4.3	適用対象の明確化
↑	↑	2023/3/27	46F 安江	4.3.3	セキュアコーディング要件の明確化(VULCMN_01200, VULCMN_50800, VULCMN_50900 削除)

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		8/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

目次

1. はじめに	9
1.1. 本書の目的	9
1.2. 本書の位置づけ $\Delta 6 \Delta 12$	9
1.3. 適用範囲 $\Delta 12$	9
1.4. 要件の記載 $\Delta 12$	9
1.5. 略語・用語解説	9
1.6. 関連文書	11
2. 本書の前提条件 $\Delta 6$	14
2.1. トヨタとサプライヤ間での CIA の締結 $\Delta 6 \Delta 15$	14
3. 脆弱性対策概要	15
3.1. 脆弱性対策概要	15
3.2. 脆弱性対策の評価概要 $\Delta 6$	22
3.3. 要件一覧 $\Delta 12$	23
3.4. 対策要件と評価要件の対応関係	26
4. 脆弱性対策・脆弱性対策の評価の要件 $\Delta 1 \Delta 6 \Delta 7$	27
4.1. 共通要件 $\Delta 6$	27
4.2. 暗号アルゴリズム・乱数の対策	28
4.2.1. 暗号アルゴリズム	28
4.2.2. 乱数	30
4.3. 車載部品非開封攻撃への耐性	36
4.3.1. 車載部品非開封の特権機能対策（デバッグ／メンテナンス）	36
4.3.2. 仕様面の対策	42
4.3.3. セキュアコーディング	45
4.3.4. プログラム／データの保護対策（プログラムの保護）	49
4.3.5. プログラム／データの保護対策（CSP・PSPの保護）	50
4.3.6. プログラム／データの保護対策（情報系車載部品のデータの保護）	54
4.4. 車載部品開封攻撃への耐性	59
4.4.1. 車載部品開封の特権機能対策（テストアクセスポート）	59
4.4.2. PCB 解析対策	61
4.4.3. 耐タンパ	63
5. （欠番） $\Delta 6 \Delta 15$	66
5.1. （欠番） $\Delta 6 \Delta 15$	66

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		9/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

1. はじめに

1.1. 本書の目的

車載部品の共通の脆弱性を低減するための最低限の脆弱性対策要件を示すこと。

1.2. 本書の位置づけ ^{Δ6Δ12}

本書と同様に、ECU を脆弱性なく作り込むための対策要件書／評価要件書と、各文書の位置づけの一覧を表 1-1 に示す。 ^{Δ6}

表 1-1 脆弱性を低減するための要件書一覧 ^{Δ6}

文書名	位置づけ
ECU 脆弱性対策要求仕様書	ECU 開発における各アーキテクチャ設計工程において、脆弱性分析／脆弱性対策を実施する際の要求事項を定義。
ECU 脆弱性対策評価仕様書	ECU 開発における各テスト工程において、セキュリティに関連する機能の評価（脆弱性評価を含む）の要求事項を定義
共通脆弱性対策要求仕様書（本書）	攻撃者による脆弱性の探索を困難にするため、設計／評価、および、実装工程で、各 ECU が共通に実施すべき脆弱性対策を定義。

1.3. 適用範囲 ^{Δ12}

トヨタでは、車両へのハッキングを防ぐため、攻撃の経路上に位置する ECU に対してセキュリティ仕様書の引き当てを指示している。本書の対象は、いずれかのセキュリティ機能の開発が指示された ECU である。

1.4. 要件の記載 ^{Δ12}

脆弱性対策によってセキュリティリスクを許容可能なレベルまで低減するためには、目標とする Attack Potential (以下、目標 AP) ^{Δ7} に応じた脆弱性対策の適用が必要となる。本書の各要件では、適用条件として以下 2 つの項目を定義している。各要件を確認し、条件に該当する要件に対応すること。 ^{Δ6}

- ① 機能/部品：特定の機能（無線通信機能など）／特定の部品（既製品など）を利用するか否か
- ② 目標 AP：各 ECU に引当たるサイバーセキュリティ要求に付与された値（※） ^{Δ11}

※目標 AP の定義は ECU 脆弱性対策要求仕様書にて記載する ^{Δ11}。

1.5. 略語・用語解説

本書で用いる略語を解説する。

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		10/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

表 1-2 略語一覧 ^{Δ12}

略語	解説
CAVP	Cryptographic Algorithm Validation Program 暗号アルゴリズム認証制度 http://csrc.nist.gov/groups/STM/cavp/

本書で用いる用語・定義語を解説する。

表 1-3 用語・定義語一覧 ^{Δ12}

用語	解説
危殆化	何らかの作為や状況の変化により、セキュリティの安全性のレベルが低下した状況。暗号鍵の漏えい、コンピュータの処理能力向上による暗号アルゴリズムの安全性低下等。
特権モード	無制限の CPU 動作を許すモード。任意の命令を実行でき、入出力操作を開始でき、全メモリ空間にアクセス可能。 別名カーネルモード、スーパバイザモード
ユーザモード	特権モード以外のモード。一部の命令が実行できなくなり、入出力操作ができなくなり、メモリ空間の一部にアクセスできなくなる。
トヨタ指示仕様 ^{Δ2}	トヨタ発行の車載部品の外設申に記載されている要件書で指示しているもの。 ^{Δ2}
認証データ ^{Δ4}	ユーザ又は情報システムの身元の信頼を確立するプロセス（認証）において、認証する者とされるものが扱うデータ。ID やパスワード、証明書が含まれる。 ^{Δ4}
乱数シード ^{Δ4}	疑似乱数生成器の入力。異なる乱数シードは異なる疑似乱数シーケンスを生成する。 ^{Δ4}
アプリ ^{Δ10}	POSIX または AGL に準拠した OS 上で動作し、お客様にサービス（決済やエンターテインメント機能等）を提供するソフトウェア

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		11/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

1.6. 関連文書

本書の関連文書を以下に示す。

表 1-4 関連文書一覧 ^{Δ1Δ5Δ6 Δ12}

仕様書番号	名称
(欠番) ^{Δ16}	
SEC-ePF-VUL-ECU-REQ-SPEC ^{Δ6}	ECU 脆弱性対策要求仕様書 ^{Δ6}
SEC-ePF-VUL-ECU-TST-SPEC ^{Δ6}	ECU 脆弱性対策評価仕様書 ^{Δ6}
wguide ^{Δ5}	ダイアグ憲法 ^{Δ2}
SEC-ePF-RPR-REQ-SPEC ^{Δ6}	標準リプログラミングセキュリティ要求仕様書
SEC-ePF-PPI-REQ-SPEC ^{Δ6}	車載個人・プライバシー情報対策要件書 ^{Δ5Δ6}
SEC-ePF-TRM-GUD-PROC ^{Δ12}	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 ^{Δ12}

※表 1-4 関連文書一覧 は今後更新予定 ^{Δ6}

表 1-5 公的関連文書一覧 ^{Δ1Δ5}

本書における略称 ^{Δ5}	名称/外部リンク
CAVP ^{Δ5}	Cryptographic Algorithm Validation Program http://csrc.nist.gov/groups/STM/cavp/
AIS20 ^{Δ5}	Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_Functionality_Classes_Evaluation_Methodology_DRNG_e.pdf?__blob=publicationFile&v=1
KS2011 ^{Δ5}	A proposal for: Functionality classes for random number generators https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile&v=1Δ4 ※AIS20 と AIS31 とを統合した文書 ^{Δ5}
AIS31 ^{Δ5}	A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		12/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

本書における略称 ^{Δ5}	名称/外部リンク
	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_evaluation_methodology_for_true_RNG_e.pdf?__blob=publicationFile&v=1
ISO/IEC TR 24772 ^{Δ5}	Information technology – Programming languages – Guidance to avoiding vulnerabilities in programming languages through language selection and use http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csn=61457
CERT-C ^{Δ5}	SEI CERT C Coding Standard https://www.securecoding.cert.org/confluence/display/c/SEI+CERT+C+Coding+Standard
CERT-C++ ^{Δ5}	SEI CERT C++ Coding Standard https://www.securecoding.cert.org/confluence/pages/viewpage.action?pageId=637
CERT-JAVA ^{Δ5}	SEI CERT Oracle Coding Standard for Java https://www.securecoding.cert.org/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java
CERT-Perl ^{Δ5}	SEI CERT Perl Coding Standard https://www.securecoding.cert.org/confluence/display/perl/SEI+CERT+Perl+Coding+Standard
ISO/SAE 21434 ^{Δ6}	ISO/SAE DIS 21434 Road vehicles — Cybersecurity engineering https://www.iso.org/standard/70918.html
ISO/IEC 19790 ^{Δ6}	Information technology – Security techniques – Security Requirements for Cryptographic Modules http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csn=52906
SP800-57 ^{Δ6}	Recommendation for Key Management: Part1 General https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
SP800-90A ^{Δ12}	Recommendation for Random Number Generation Using Deterministic Random Bit Generators https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		13/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

本書における略称 ^{Δ5}	名称/外部リンク
SP800-90B ^{Δ12}	Recommendation for the Entropy Sources Used for Random Bit Generation https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf
SP800-140C ^{Δ6}	CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140C.pdf
SP800-140D ^{Δ6}	CMVP Approved Sensitive Security Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140D.pdf
FIPS	Federal Information Processing Standards https://csrc.nist.gov/publications/fips
WP29 ^{Δ6}	A new UN Regulation on Cyber security https://www.unece.org/trans/main/wp29/meeting_docs_grva.html

(注 1)

最新の仕様書の内容に従うこと

(注 2)

本書とその関連仕様書、トヨタ各設計が発行する仕様書に記載された内容との間に相違がある場合には、関係者間でその内容を確認する必要があるため、セキュリティ主管部署（本仕様書発行部署）と確認対象の仕様書を発行するトヨタ各設計に連絡すること

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		14/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

2. 本書の前提条件 ^{Δ6}

本書では、ECU を脆弱性なく作りこむための要件を定義する。

2.1. トヨタとサプライヤ間での CIA の締結 ^{Δ6Δ15}

ECU の開発を開始する際に、トヨタはサプライヤに外注品設計申入書（以降、外設申と記載）を発行し、ECU に対して引き当てる仕様書（セキュリティに関連する仕様書を含む）を指示している。 ^{Δ6}

ISO/SAE 21434 に準拠するため、外設申の発行までに、トヨタとサプライヤ間の役割／責任分担を明確化し、CIA（Cybersecurity Interface Agreement） ^{Δ15} を締結している。締結した CIA ^{Δ15} は、セキュリティに関連する仕様書と合わせて外設申に添付している。 ^{Δ6}

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		15/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

3. 脆弱性対策概要

3.1. 脆弱性対策概要

セキュリティ機能を必要とする機器は、解析・攻撃に曝される可能性がある。一般に、攻撃者はセキュリティシステムを攻撃する際、まず機器の解析を行い、脆弱なポイントがないか探る。その上で脆弱性を利用し、実攻撃を行う。

解析・攻撃のリスクを軽減するためには、セキュリティ機能を設計・実装する上で、攻撃者に活用される脆弱性を少なく設計・実装することと、攻撃者が脆弱性の探索を困難にする、すなわち解析しにくい設計・実装が重要となる。

本要件書は、脆弱性の低減と解析の抑止を目的として記載している。

下図（図 3-1）に車載部品(ECU)の解析・攻撃の入口をモデル化したものを示す。車載部品に格納されたプログラムとデータを保護資産と仮定し、どのような解析・攻撃があるかを示す。

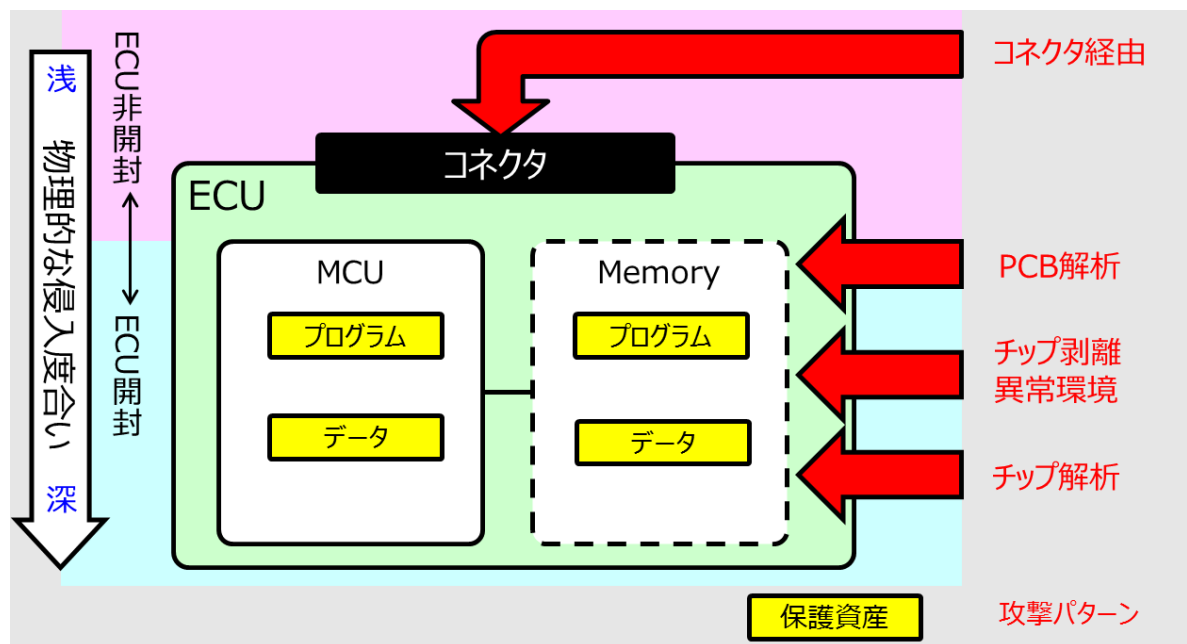


図 3-1 車載部品(ECU)に対する解析・攻撃の入口

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		16/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

各解析・攻撃の入口と概要、説明を表 3-1 に示す。

表 3-1 各解析・攻撃の入口と概要、説明

入口		概要	説明
車載部品 非開封 (解析・ 攻撃)	コネクタ 経由	暗号アルゴリズム・ 乱数の不備の利用	・暗号アルゴリズム仕様、乱数仕様の選定時の考慮 不足、それらが正しく動かないことを利用した 解析・攻撃
		特権機能の利用	車載部品境界面のコネクタ、無線に接続された特権 機能、もしくはグローバルバス経由で接続された特権 機能からの以下の解析・攻撃 $\Delta 4$ ・ダイアグによるデータアクセス (読出し／書き換え) ・CAN 等のキャリブレーションによるアクセス (読出し／書き換え) ・リプログラミング機能によるプログラム書き換え ・サプライヤの製品検査用機能による情報資産への アクセス ・外部からコマンド実行可能な IP サービス $\Delta 9$
		ソフトウェア解析	・ソフトウェア実装上の脆弱性を悪用した、処理の 乗っ取り、不正プログラム注入、内部情報の解析等
車載部品 開封 (解析)	PCB 解析	特権機能の利用	・テストアクセスポート (JTAG 等) 利用、解析・ 書き換え ・マイコンテストモード利用、解析・書き換え
		PCB 表層プローブ	・配線のプロービング：チップ間通信の盗聴、解析 ・端子から侵入、データ読出し・書き換え
	チップ 剥離	チップ交換	・チップ交換によるプログラム書き換え ・基板から剥がして解析
	異常環境	ノイズ注入 (フォールト攻撃)	・レーザ照射、ノイズ注入し、誤動作させて解析
	チップ 解析	サイドチャネル 攻撃	・チップ外部からの電磁波、電流測定等による暗号鍵 の推定
		チップ破壊解析 (侵襲攻撃)	・チップの破壊解析、電子顕微鏡による解析、 シリコンダイのプロービング

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		17/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

各解析・攻撃概要と対策概要の対応関係を表 3-2 に示す。

表 3-2 各解析・攻撃概要と対策概要の対応関係

対策概要		暗号アルゴリズム・乱数の対策	車載部品非開封の特権機能対策 (デバッグ/メンテナンス)	仕様面の対策	セキュアコーディング	プログラム/データの保護対策	車載部品開封の特権機能対策(テストアクセスポート)	PCB 解析対策	耐タンパ
解析・攻撃概要									
車載部品 非開封 (解析・ 攻撃)	暗号アルゴリズム・乱数の不備の利用	○							
	特権機能の利用		○			○			
	ソフトウェア解析			○	○	○			
車載部品 開封 (解析)	特権機能の利用					○	○		
	PCB 表層プローブ					○		○	
	チップ交換					○			
	ノイズ注入								○
	サイドチャネル攻撃								○
	チップ破壊解析								○

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		18/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

以降に、解析・攻撃の入口に対する解析・攻撃（以降の内容では、「解析・攻撃」をまとめて「攻撃」と記載）と対策を説明する。車載部品は目標 AP^{Δ7}に応じた対策を行なわなければならない。

コネクタ経由

■攻撃：暗号アルゴリズム・乱数の不備の利用

暗号アルゴリズム仕様、乱数仕様の選定時の考慮不足や正しく動作しないことを利用される可能性があるがあるので対策しなければならない。

◇対策：暗号アルゴリズム・乱数の対策

脆弱性が無いことが確認されているトヨタ指定の暗号アルゴリズム、乱数を選定し、又、車載部品で正しく動くことを確認すること。

■攻撃：車載部品非開封の特権機能の利用（デバッグ／メンテナンス）

特権機能とは、車載部品に格納されたプログラム、データにアクセス ^{Δ4}できるデバッグ／メンテナンス機能のことである。車載部品非開封の特権機能には、車載部品境界面のコネクタに特権機能を接続する場合、グローバルバス経由で特権機能を接続する場合、もしくは無線通信経由で特権機能を接続する場合が該当する。^{Δ4Δ9}

車載部品非開封の特権機能としては、上記場合の ^{Δ4} ダイアグ ^{Δ4} によるメモリの Read/Write、CCP/XCP^{Δ7}によるデータの読出し/書き換え、リプログラミングによるプログラムの書き換え、外部からコマンド実行可能な IP サービス(telnet, ssh, dbus, Android Debug Bridge 等)^{Δ9}による外部からの操作 ^{Δ16}、サプライヤの製品検査用機能による情報資産へのアクセスが該当する。

本機能は開発・製造・メンテナンス・不良解析・廃棄と各ライフサイクルで使用される重要な機能であるが、攻撃者から見れば非常に強力なバックドアとなり、プログラムやデータの読出し、暗号鍵の読出しや書き換え、プログラム改ざんによるセキュリティ機能の無効化等の攻撃に利用できる可能性がある所以对策しなければならない。

◇対策：車載部品非開封の特権機能対策（デバッグ／メンテナンス）

特権機能の無効化、又は認証によるアクセス権の管理を行う。

なお、認証に用いる暗号鍵が全ての車載部品で共通の場合、1つの車載部品で暗号鍵が漏えいすると他の車載部品にも影響が拡大する。目標 AP^{Δ7}に応じて車両別に異なる暗号鍵を利用する、車両内の全車載部品で異なる暗号鍵を利用する等、他車両に影響が出ないように考慮すること。

◇対策：プログラム／データの保護対策 ^{Δ12}

プログラム実行・データ使用をする前に完全性を確認することで、改ざんされたことを検知することができる。リプログラミング機能搭載車載部品は確実に対応すること。

また、特権機能が攻撃者に悪用されないように、セキュアマイコン等を利用することで、プログラム

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		19/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

とデータ（特に CSP・PSP^{Δ7}：暗号鍵等）を保護することが可能であるので目標 AP^{Δ7} に応じて対策すること。

3 章以降の対策説明では、車載部品非開封攻撃のプログラム／データ保護にマージする。

■攻撃：ソフトウェア解析

ソフトウェアの実装や OS／ハードの設定に不備がある場合、脆弱性を利用してプロセスの乗っ取りや不正プログラムの注入、権限の昇格等の攻撃が行われる可能性があるので対策しなければならない。

◇対策：仕様面の対策

ソフトウェアの機能を明確化し、余計な機能を盛り込まないことで、脆弱性が存在しうる機能の混入を防止すること。

◇対策：セキュアコーディング

ソフトウェア実装時、攻撃者に利用され得る脆弱性を盛り込まないように、セキュアコーディングルールに従い実装を行い、脆弱性の混入を防止すること。

◇対策：プログラム／データの保護対策

対策の説明については、前述のコネクタ経由の「プログラム／データの保護対策」と同じ。

PCB 解析

■攻撃：車載部品開封の特権機能の利用（テストアクセスポート）

マイコンはデバッグやメンテナンス、製造を目的とした JTAG 等のテストアクセスポートを持つ。本機能は IEEE で標準化され、マイコン内のリソースに直接アクセスできるため、攻撃者から見れば強力なバックドアとなり、プログラムやデータの読出し、暗号鍵の読出しや書き換え、プログラム改ざんによるセキュリティ機能の無効化等の攻撃に利用できる可能性があるので対策しなければならない。

◇対策：プログラム／データの保護対策

対策の説明については、前述のコネクタ経由の「プログラム／データの保護対策」と同じ。

◇対策：車載部品開封の特権機能対策（テストアクセスポート）

特権機能の無効化、又は認証によるアクセス権の管理を行う。一般に、マイコンのテストアクセスポートはパスワードによる認証機能が搭載されている場合が多い。パスワードが全ての車載部品で共通の場合、1 つ漏えいすると他の車載部品にも影響が出てしまう。全車載部品で個別の予測されづらいパスワードを設定すること。目標 AP^{Δ7} に応じて対策すること。

■攻撃：PCB 表層プローブ

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		20/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

基板表層から配線をプローブして盗聴、チップの端子、もしくは端子につながるポイントからチップへアクセスし、動作の解析や読出し・書き換えを行う攻撃が考えられる。特に外部メモリ（Flash 等）にプログラムを格納する場合、端子から容易に読出し、書き換えができる可能性があるので対策しなければならない。

◇対策：プログラム／データの保護対策

対策の説明については、前述のコネクタ経由の「プログラム／データの保護対策」と同じ。

◇対策：PCB 解析対策

チップ間通信は機密情報の解析を防ぐために通信内容を暗号化すること。何らかの制約により外部メモリに CSP^{A4} を格納する場合、マイコンで暗号化して格納すること。また全ての通信内容を秘匿する必要はなく、機密情報（ここでは、CSP^{A4}）の漏えいにつながる場合や、セキュリティ機能の解析につながる場合のみで良い。目標 AP^{A7} に応じて対策すること。

チップ剥離

■攻撃：チップ交換

外部メモリにプログラムを格納している場合、外部メモリチップ交換によりプログラムを改ざんされる可能性があるので対策しなければならない。

◇対策：プログラム／データの保護対策

対策の説明については、前述のコネクタ経由の「プログラム／データの保護対策」と同じ。

異常環境

■攻撃：ノイズ注入攻撃

レーザ照射やクロックのグリッチ、電圧低下等でチップを誤動作させ、プログラムの IF 文分岐を正しく動作させないことで、でたらめな値でも認証を成功させてしまうような攻撃があるので対策しなければならない。

◇対策：耐タンパ

ノイズ検出、レイアウト等による物理解析への耐性、サイドチャネル攻撃への耐性が対策となるので、目標 AP^{A7} に応じて対策すること。

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		21/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

チップ解析

■攻撃：サイドチャネル攻撃

暗号処理中の電磁波や消費電流を測定し、統計処理することで暗号鍵を推定する攻撃があるので対策しなければならない。

◇対策：耐タンパ^{Δ1}

対策の説明については、前述の異常環境の対策と同じ。^{Δ1}

■攻撃：チップ破壊解析

チップを破壊し、レイアウトや配線情報を電子顕微鏡等で観察することで処理内容を解析又は ROM を読み取る、シリコンダイの配線を直接プローブすることで機密情報の読み取りを行う、FIB 加工で回路を改変する等の攻撃もあるので対策しなければならない。

◇対策：耐タンパ

対策の説明については、前述の異常環境の対策と同じ。

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		22/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

3.2. 脆弱性対策の評価概要 ^{Δ6}

脆弱性対策を行った製品は、適切に対策が実装され、許容できない脆弱性が含まれていないことを評価する必要がある。脆弱性対策の評価とは、各脆弱性対策について、設計検証、ソースコードレビュー等を実施し、設計や実装に対策が正確に反映されているかどうかを確認することである。脆弱性対策概要に対応する脆弱性対策の評価概要を表 3-3 に示す。 ^{Δ6}

表 3-3 脆弱性対策の評価概要 ^{Δ1Δ6}

脆弱性対策概要	脆弱性対策の評価概要 ^{Δ1Δ6}
暗号アルゴリズム・乱数の対策	暗号アルゴリズム・乱数基準テスト
車載部品非開封の特権機能対策 (デバッグ／メンテナンス)	車載部品非開封の特権機能対策 (デバッグ／メンテナンス) チェック
仕様面の対策	仕様面の対策チェック
セキュアコーディング	セキュアコーディングチェック
プログラム／データの保護対策	プログラム／データの保護対策チェック
車載部品開封の特権機能対策 (テストアクセスポート)	車載部品開封の特権機能対策 (テストアクセスポート) チェック
PCB 解析対策	PCB 解析対策チェック
耐タンパ	耐タンパチェック

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		23/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

3.3. 要件一覧 ^{△12}

本書で規定する要求一覧を表 3-4 に示す。各要求の詳細は 4 章以降を参照。

また、ハードウェア選定時に参照すべき要求事項を「ハードウェア関連要求」列に「○」で示す。

表 3-4 要件一覧

分類	要求事項	ハードウェア 関連要求
共通要件	VULCMN_52400(欠番)	-
暗号アルゴリズム・乱数の対策	VULCMN_00100	-
	VULCMN_03600	-
	VULCMN_50100	-
	VULCMN_52500	-
	VULCMN_00200	○
	VULCMN_00300	-
	VULCMN_50200	-
	VULCMN_50300	-
車載部品非開封攻撃への耐性	VULCMN_00400	-
	VULCMN_00500	-
	VULCMN_00501	-
	VULCMN_00502	-
	VULCMN_00503	-
	VULCMN_00600(欠番)	-
	VULCMN_00700	-
	VULCMN_00800	-
	VULCMN_00900	-
	VULCMN_50400	-
	VULCMN_50500	-
	VULCMN_01000	-
	VULCMN_01100	-
	VULCMN_50600	-
	VULCMN_50700	-
	VULCMN_01200	-
	VULCMN_01300	-
	VULCMN_50800	-
	VULCMN_50900(欠番)	-

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		24/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

	VULCMN_51000	-
	VULCMN_01400	-
	VULCMN_01500(欠番)	-
	VULCMN_51100	-
	VULCMN_01600	-
	VULCMN_01700	○
	VULCMN_01701	-
	VULCMN_01702	○
	VULCMN_01800	-
	VULCMN_01900	-
	VULCMN_02000(欠番)	-
	Δ13	
	VULCMN_51200	-
	VULCMN_02100	-
	VULCMN_02200	-
	VULCMN_02300	-
	VULCMN_02400(欠番)	-
	VULCMN_03700	-
	VULCMN_03800	-
	VULCMN_03900	-
	VULCMN_04000	-
	VULCMN_51300	-
	VULCMN_51400	-
	VULCMN_51500(欠番)	-
	VULCMN_52600	-
	VULCMN_52700	-
	VULCMN_52800	-
	VULCMN_52900	-
車載部品開封攻撃への耐性	VULCMN_02500	-
	VULCMN_02501	-
	VULCMN_02502	-
	VULCMN_02503	-
	VULCMN_02600	-
	VULCMN_02601	-
	VULCMN_02602	○

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		25/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

	VULCMN_51600	-
	VULCMN_51700	-
	VULCMN_02700	○
	VULCMN_02800	-
	VULCMN_51800	-
	VULCMN_51900	-
	VULCMN_02900	○
	VULCMN_03000	○
	VULCMN_03100(欠番)	○
	VULCMN_03200	○
	VULCMN_03300	○
	VULCMN_03400	○
	VULCMN_03500	○
	VULCMN_52000	-
	VULCMN_52100(欠番)	-
	VULCMN_52200	-
既製品に対するセキュリティ評価	VULCMN_52300(欠番)	-

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		26/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

3.4. 対策要件と評価要件の対応関係

対策要件と共に評価要件が4章に記載されている。これらの要件項目にはIDが割り当てられており、対策要件と評価要件の対応が取れるようになっている。全ての対策要件に対して評価を必ず実施すること。

対策要件と評価要件の対応関係を表 3-5 に示す。

表 3-5 対策要件と評価要件の対応関係 ^{Δ6}

脆弱性対策概要	対策要件(ID)	評価要件(ID)
暗号アルゴリズム・乱数の対策	VULCMN_00100, VULCMN_00200, VULCMN_00300, VULCMN_03600 ^{Δ16}	VULCMN_50100 ^{A4} , VULCMN_50200 ^{A4} , VULCMN_50300 ^{A4} , VULCMN_52500 ^{Δ16}
車載部品非開封の特権機能対策 (デバッグ／メンテナンス)	VULCMN_00400, VULCMN_00500, VULCMN_00501, VULCMN_00502, VULCMN_00503, VULCMN_00700, VULCMN_00800, VULCMN_00900	VULCMN_50400 ^{A4} , VULCMN_50500
仕様面の対策	VULCMN_01000, VULCMN_01100	VULCMN_50600 ^{A4} , VULCMN_50700 ^{A4}
セキュアコーディング	VULCMN_01200, VULCMN_01300	VULCMN_50800, VULCMN_51000 ^{A4}
プログラム／データの保護対策	VULCMN_01400, VULCMN_01600, VULCMN_01700, VULCMN_01701, VULCMN_01702, VULCMN_01800, VULCMN_01900, VULCMN_02100, VULCMN_02200, VULCMN_02300, VULCMN_03700 ^{A9} , VULCMN_03800 ^{A9} , VULCMN_03900 ^{Δ10} , VULCMN_04000 ^{Δ10}	VULCMN_51100 ^{A4} , VULCMN_51200 ^{A4} , VULCMN_51300 ^{A4} , VULCMN_51400 ^{A4} , VULCMN_52600 ^{A9} , VULCMN_52700 ^{A9} , VULCMN_52800 ^{Δ10} , VULCMN_52900 ^{Δ10}
車載部品開封の特権機能対策 (テストアクセスポート)	VULCMN_02500, VULCMN_02501, VULCMN_02502, VULCMN_02503, VULCMN_02600	VULCMN_51600, VULCMN_51700
PCB 解析対策	VULCMN_02700, VULCMN_02800	VULCMN_51800 ^{A4} , VULCMN_51900 ^{A4}
耐タンパ	^{Δ5} VULCMN_02900, VULCMN_03000, VULCMN_03200, VULCMN_03300, VULCMN_03400, ^{Δ6} VULCMN_03500 ^{Δ6}	^{Δ5} VULCMN_52000 ^{A4} , VULCMN_52200 ^{Δ6}

注) 詳しくは 5 章以降の各要件項目を確認すること。

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		27/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

4. 脆弱性対策・脆弱性対策の評価の要件 ^{Δ1Δ6Δ7}

本章では、脆弱性対策・脆弱性対策の評価の要件を示す。

各要件の適用について、まず、各要件の適用条件を確認する。ECU が適用条件を満たす場合、当該要件の目標 AP を確認する。ECU の搭載するセキュリティ機能の目標 AP が当該要件の目標 AP に当て嵌まる場合、ECU に当該要件を適用する。(以下、ECU に適用した要件を適用要件と記す)^{Δ7}

4.1. 共通要件 ^{Δ6}

本節では、本章で定める要件で共通の要件事項を示す。

エビデンスの作成期限についての要件事項 ^{Δ6}

ID		VULCMN_52400
適用条件 ^{Δ12}	機能/部品	-
	目標 AP ^{Δ7}	-
要件		(欠番)

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		28/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.2. 暗号アルゴリズム・乱数の対策

セキュリティの大前提となる暗号アルゴリズムと乱数の実装について、対策要件と評価要件を示す。

4.2.1. 暗号アルゴリズム

4.2.1.1. 対策要件

暗号アルゴリズムの脆弱性を利用した攻撃を防ぐこと

ID		VULCMN_00100A ⁶
適用条件 Δ6Δ12	機能/部品	暗号アルゴリズムを使用する ECU
	目標 AP ⁷	全て Δ4Δ5Δ7
要件 Δ ⁶		<p>使用する暗号アルゴリズムは「FIPS」、「SP800-140C」、「SP800-140D」のいずれかに記載されているもののうち、Status が Final の暗号アルゴリズムを選定すること。(*1)</p> <p>*1)Status が Withdrawn, Draft のものは選定しないこと Δ⁷</p> <p>また、「SP800-57」にもとづき、セキュリティ強度が 128bit 以上を満たすように使用する暗号アルゴリズム、および鍵長を決めること。</p> <p>(補足) 以下、代表的な共通鍵暗号、公開鍵暗号、MAC に対しセキュリティ強度 128bit となる鍵長を示す。</p> <ul style="list-style-type: none"> ・共通鍵暗号 : AES/128bit ・公開鍵暗号 : RSA/3072bit, ECDSA/256bit, ECDH/256bit ・MAC : AES-CMAC/128bit <p>また、セキュリティ強度 128bit となる代表的なハッシュ関数を以下に示す。</p> <ul style="list-style-type: none"> ・ハッシュ関数 : SHA256
理由		<p>独自のアルゴリズムを使用することで、実質的な暗号強度が同じ鍵長の他の暗号アルゴリズムよりも大きく劣る場合がある。「WP29」においても、広く認められた標準規格の利用が要求されており、セキュリティ専門家の評価を十分に受けた暗号アルゴリズムのみを使用する必要がある。Δ⁶</p> <p>暗号アルゴリズムが脆弱でないことはセキュリティ機能の大前提となる。</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		29/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

ID		VULCMN_03600 ^{Δ9}
適用条件 ^{Δ12}	機能/部品	サイバーセキュリティ要求に紐づく機密性が求められる暗号鍵(共通鍵、秘密鍵)を暗号処理に使用する ECU
	目標 AP	全て
要件		機密性が求められる同一の暗号鍵を複数目的の暗号処理に使用しないこと
理由		同一の暗号鍵を複数の用途に扱うことで、暗号鍵の漏洩の可能性、さらには漏洩時の影響の広がり懸念されるため

4.2.1.2. 評価要件

ID		VULCMN_50100 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	暗号アルゴリズムを使用する ECU
	目標 AP ^{Δ4Δ7}	全て ^{Δ4Δ5Δ6Δ7}
要件		<p>本要件は VULCMN_00100 を適用する場合に実施すること</p> <p>暗号アルゴリズムが正しく実装されていることを確認するために、CAVP で公開されている test vector による既知解テスト(暗号アルゴリズムが AES の場合、AESAVS) ^{Δ12} 相当の試験(*)を実施すること ^{Δ4}</p> <p>*) ベンダから提供される暗号モジュールを使用する場合は、以下のいずれかを実施すること ^{Δ4}</p> <ul style="list-style-type: none"> ・ベンダから CAVP 相当の試験を実施した結果を受領する ^{Δ4} ・暗号モジュールに対して CAVP 相当の試験を実施する ^{Δ4}
確認内容		アルゴリズムの正当性

ID		VULCMN_52500 ^{Δ9}
適用条件 ^{Δ12}	機能/部品	VULCMN_03600 を適用した場合
	目標 AP	全て
要件		対策要件が満たされていることを設計検証により確認すること
確認内容		<p>検証対象となる暗号鍵の一覧</p> <p>上記一覧の全暗号鍵が対策要件を満たしていることを確認</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		30/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.2.2. 乱数

4.2.2.1. 対策要件

乱数の脆弱性を利用した攻撃を防ぐこと

ID		VULCMN_00200 ^{Δ6}																										
適用条件 Δ6Δ12	機能/部品	乱数生成器を搭載する ECU ^{Δ7}																										
	目標 AP ^{Δ7}	全て Δ4Δ5Δ7																										
要件		乱数生成器は下記①もしくは②の要件を満たすこと。 Δ12																										
		①: Δ12																										
		・ハードウェアの真性乱数生成器が搭載されている場合は、ハードウェアの真性乱数生成器を使用すること(*1) Δ5。ただし、真性乱数生成器は AIS31 (PTG.2 または PTG.3) Δ12 に準拠していること。																										
		・*1) ハードウェアの真性乱数生成器の出力を直接使用できない場合は、その出力を乱数シードとして疑似乱数生成器を使用してもよい。 Δ5																										
		・疑似乱数生成器を使用する場合は、AIS20 を参考に、下記目標 AP に応じた要求値を満たすこと。																										
		<table><tr><th rowspan="2"></th><th rowspan="2">乱数用途 Δ3</th><th colspan="3">目標 AP^{Δ8}</th></tr><tr><th>10～13</th><th>14～19</th><th>20</th></tr><tr><td rowspan="2">エントロピー 要求値 (ビット) Δ4</td><td>鍵生成 Δ3</td><td>-Δ3</td><td>80Δ3</td><td>80Δ3</td></tr><tr><td>C&R 認証 Δ3</td><td>(*2)に従って 決定 Δ3Δ10</td><td>(*2)に従って 決定 Δ3Δ10</td><td>(*2)に従って 決定 Δ3Δ10</td></tr><tr><td rowspan="2">アルゴリズム 予測不可能性 要求値</td><td>鍵生成 Δ5</td><td colspan="3">Backward Secrecy & Forward Secrecy(*3) Δ5</td></tr><tr><td>C&R 認証 Δ5</td><td colspan="3">Forward Secrecy(*4)Δ5Δ13</td></tr></table>		乱数用途 Δ3	目標 AP ^{Δ8}			10～13	14～19	20	エントロピー 要求値 (ビット) Δ4	鍵生成 Δ3	-Δ3	80Δ3	80Δ3	C&R 認証 Δ3	(*2)に従って 決定 Δ3Δ10	(*2)に従って 決定 Δ3Δ10	(*2)に従って 決定 Δ3Δ10	アルゴリズム 予測不可能性 要求値	鍵生成 Δ5	Backward Secrecy & Forward Secrecy(*3) Δ5			C&R 認証 Δ5	Forward Secrecy(*4)Δ5Δ13		
					乱数用途 Δ3	目標 AP ^{Δ8}																						
			10～13	14～19		20																						
		エントロピー 要求値 (ビット) Δ4	鍵生成 Δ3	-Δ3	80Δ3	80Δ3																						
			C&R 認証 Δ3	(*2)に従って 決定 Δ3Δ10	(*2)に従って 決定 Δ3Δ10	(*2)に従って 決定 Δ3Δ10																						
アルゴリズム 予測不可能性 要求値	鍵生成 Δ5	Backward Secrecy & Forward Secrecy(*3) Δ5																										
	C&R 認証 Δ5	Forward Secrecy(*4)Δ5Δ13																										
(本要件は、開発時に設計で対応するものである) Δ6																												
*2) 設計者は認証失敗時のペナルティの有無を選択し、下記の式を満たすエントロピーおよびペナルティを設定すること																												
ペナルティ無しの場合																												
H: エントロピー[bit]																												
T: C&R 認証のチャレンジ要求からチャレンジ応答までの処理時間 (1 回あたりの平均処理時間) [ms]																												
c: 単位換算係数 (1000×60×60×24×365)																												
とすると																												

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		31/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

	$H \geq \max_{1 \leq x \leq 24} \left\{ \log_2 \frac{365x(25-x)c}{T} + 1 \right\}$ <p>例) $T = 1\text{ms}$ の場合、$H \geq 51.7\text{bit}$で上記式を満足する。</p> <p>ペナルティ有りの場合</p> <p>H: エントロピー [bit]</p> <p>T: C&R 認証のチャレンジ要求からチャレンジ応答までの処理時間 (1 回あたりの平均処理時間) [ms]</p> <p>T': C&R 認証のチャレンジ要求からチャレンジ応答までの処理時間 (ペナルティ時間を含んだ 1 回あたりの平均処理時間) [ms]</p> <p>N: ペナルティが発生するまでの認証失敗回数 [回]</p> <p>P: ペナルティによるウエイト時間 [ms]</p> <p>c: 単位換算係数 ($1000 \times 60 \times 60 \times 24 \times 365$)</p> <p>とすると</p> $H \geq \max_{1 \leq x \leq 24} \left\{ \log_2 \frac{365x(25-x)c}{T'} + 1 \right\}$ $T' = (N \cdot T + P) / N$ <p>例) $T = 1\text{ms}$、$H = 40\text{bit}$ の場合、$N \leq 3$回、$P \geq 10$秒のペナルティで上記式を満足する。^{Δ10}</p> <p>*3) Backward Secrecy と Forward Secrecy については、AIS20 - K3 と同等の KS2011 - DRG.2 を参照^{Δ5}</p> <p>*4) Forward Secrecy については、KS2011 - DRG.1 を参照^{Δ13}</p> <p>・乱数用途が上表のものに当て嵌まらない場合には、該当する目標 AP で最大のエントロピー要求値とアルゴリズム予測不可能性要求値で設計すること。^{Δ3Δ5}</p> <p>・エントロピー要求値とアルゴリズム予測不可能性要求値が上表のものに満たない場合は、代替の対策要件で対応できないかについて、システム担当 (各設計)、部品担当 (各設計)、セキュリティ主管部署 (本仕様書発行部署) 及びサプライヤで協議を行なうこと。^{Δ3Δ5}</p> <p>・乱数が一定以上の確率で異なる値で出力される設計とするために、下記表を参考に、乱数が KS2011 - DRG.2.4 の要件を満たすことを確認すること。なお、VULCMN_00100 の要件を満たした暗号アルゴリズムを使用している場合は、KS2011 - DRG.2.4 の要件を満たしているものとする。^{Δ13Δ14}</p>								
	<table border="1"> <tr> <th rowspan="2"></th><th colspan="3">目標 AP</th></tr> <tr> <th>10～13</th><th>14～19</th><th>20</th></tr> </table>				目標 AP			10～13	14～19
	目標 AP								
	10～13	14～19	20						

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		32/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

		(AVA_VAN.2)	(AVA_VAN.3)	(AVA_VAN.4)
	128bit 乱数列衝突の要件 k: 128bit 乱数列の個数 ε: 衝突確率	$k > 2^{14}$ and $\varepsilon < 2^{-8}$	$k > 2^{19}$ and $\varepsilon < 2^{-10}$	$k > 2^{26}$ and $\varepsilon < 2^{-12}$
<p>② : Δ12</p> <p>SP800-90B に準拠したエントロピー源の出力を乱数シードとして、SP800-90A に準拠した擬似乱数生成器を使用すること。Δ14</p> <p>なお、擬似乱数生成器は以下を満たすこと。</p> <ul style="list-style-type: none"> ・セキュリティ強度(*5) : 128bit 以上 <p>(補足) 擬似乱数生成アルゴリズム(*5) : Hash_DRBG, HMAC_DRBG, CTR_DRBG のうち任意の方式を採用してもよい。ただし CTR_DRBG を採用する場合は、利用するブロック暗号は AES とすること。</p> <p>*5)セキュリティ強度、擬似乱数生成アルゴリズムについては、SP800-90A を参照 Δ14</p>				
理由	<p>乱数性が低いことで認証機能が脆弱になる可能性がある。</p> <p>乱数生成はセキュリティの大前提のため、全目標 AP で適用とする。</p> <p>ただし、乱数はその用途や脅威によって必要なエントロピーとアルゴリズム予測不可能性が異なるため、目標とするエントロピーとアルゴリズム予測不可能性を製品ごとに設定する必要がある。Δ5</p> <p>ハードウェアの真性乱数生成器が搭載されている場合、パフォーマンス上の問題が無ければハードウェアの機能を使うことで、十分な乱数性を持つ乱数を得られる。</p> <p>上記計算式における 365 は 1 年あたりに入手できるチャレンジとレスポンスの正しい組み合わせの数を表しており、25 は車両の耐用年数を表している。</p>			

乱数値を固定化されるような攻撃を防ぐこと

ID		VULCMN_00300Δ6
適用条件 Δ6Δ12	機能/部品	乱数生成器を搭載する ECUΔ7
	目標 APΔ7	全て Δ4Δ5Δ7
要件		<p>乱数生成器より以下の乱数が出力された場合、その乱数は使用しないこと</p> <ul style="list-style-type: none"> ・ ALL0 (乱数ビット列の全てのビットが 0) Δ4 ・ ALL1 (乱数ビット列の全てのビットが 1) Δ4 ・ 前回の乱数と同じ乱数(*) <p>(本要件は、開発時ではなく、市場での乱数への攻撃を想定した物である)</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		33/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

	<p>*)ECU リセット後、最初に乱数を使用する際は、以下によりリセット前の乱数の記憶を回避してもよい。^{Δ7}</p> <p>リセット後、乱数を2回連続で生成し、2回目に生成した乱数が、1回目に生成した乱数(前回の乱数)と異なることを確認後、2回目に生成した乱数を使用する。^{Δ7}</p>
理由	乱数を固定化する攻撃を受けると、上記のような乱数が出力され、乱数の意味をなさなくなってしまうため。

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		34/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.2.2.2. 評価要件

ID		VULCMN_50200 ^{△6}
適用条件 △6△12	機能/部品	乱数生成器を搭載する ECU ^{△7}
	目標 AP ^{△7}	全て △4△5△7
要件		<p>本要件は VULCMN_00200 を適用する場合に実施すること</p> <p>真性乱数生成器を使用する場合は、AIS31 の基準を、擬似乱数生成器を使用する場合は、AIS20 の基準を満たす乱数であることを乱数基準テストにより確認すること。もしくは乱数生成器を構成する擬似乱数生成器、エントロピー源がそれぞれ SP800-90A, SP800-90B の基準を満たすことを確認すること。</p> <p>△12 (*1)^{△4}</p> <p>*1) ベンダから提供される乱数生成器を使用する場合は、以下のいずれかを実施すること。△4</p> <ul style="list-style-type: none"> ・ベンダから AIS20, AIS31 の乱数基準テストを実施した結果を受領する △4。 ・もしくは SP800-90A, SP800-90B[△] の乱数基準テストを実施した結果を受領する。△12 ・乱数生成器に対して AIS20, AIS31 の乱数基準テストを実施する。△4(*2) ・もしくは SP800-90A, SP800-90B の乱数基準テストを実施する。△12(*3) <p>*2) 乱数基準テストの実施方法は、KS2011 2.4.3. Standard Statistical Tests 及び 2.4.4. Test procedures を参照すること。△7</p> <p>C&R 認証においてペナルティ有りを選択した場合、ペナルティ要件が満たされていることを機能テストにより確認すること。△10</p> <p>*3) 乱数基準テストの実施方法は、CAVP の公開する Test Vecotrs、SP800-90A 11.Assurance, SP800-90B 3.Entropy Source Validation 以降に記載のテストを参照すること。△12</p>
確認内容		乱数性、ペナルティ対策の正当性 △10

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		35/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

ID		VULCMN_50300 ^{Δ6}
適用条件 Δ6Δ12	機能/部品	乱数生成器を搭載する ECU ^{Δ7}
	目標 AP ^{Δ4Δ7}	全て Δ4Δ5Δ7
要件		本要件は VULCMN_00300 を適用する場合に実施すること 対策要件が満たされていることを機能テストにより確認すること。機能テストが実施できない場合は、機能仕様のデザインレビュー ^{Δ4} により確認すること。
確認内容		対策実施の有無 対策の正当性

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		36/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

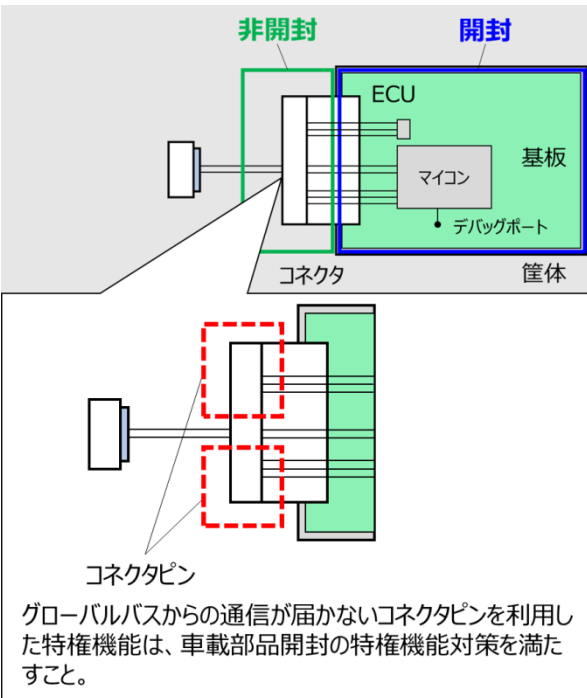
4.3. 車載部品非開封攻撃への耐性

車載部品非開封の攻撃としては、本来の機能の脆弱性をついた攻撃と、直接車載部品内メモリにアクセスできる特権機能を用いた攻撃がある。それぞれに対する対策要件と評価要件を示す。

4.3.1. 車載部品非開封の特権機能対策（デバッグ／メンテナンス）

4.3.1.1. 対策要件

車載部品非開封で利用できる特権機能を悪用した攻撃を防ぐこと ^{Δ7}

ID		VULCMN_00400 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	車載部品非開封で利用できる特権機能を設置する ECU ^{Δ7}
	目標 AP ^{Δ7}	全て ^{Δ4Δ5Δ7}
要件		<p>トヨタのセキュリティ主管部署が許可している機能以外の ^{Δ2} 特権機能を設置 ^{Δ2} する場合は、製品出荷前にその特権機能 ^{Δ4} を取り除くこと。(*1)^{Δ4}</p> <p>セキュリティ主管部署が許可している特権機能を以下に示す。 ^{Δ12}</p> <ul style="list-style-type: none"> ・標準リプログラミング機能 ・OTA リプログラミング機能 ^{Δ15} <p>ただし、グローバルバスからの通信で利用できない有線 I/F を介した ^{Δ9} 特権機能（図 3-2-1 の点線枠内のコネクタピンを利用したもの）は、「4.4.1 車載部品開封の特権機能対策（テストアクセスポート）」の要件を満たせば、残置を許可する。 ^{Δ2}</p>
		 <p>コネクタピン</p> <p>グローバルバスからの通信が届かないコネクタピンを利用した特権機能は、車載部品開封の特権機能対策を満たすこと。</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		37/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

	<p>図 3-2-1 グローバルバスからの通信が届かないコネクタピン ^{Δ2}</p> <p>対策実施時期：遅くとも 1A の製品出荷前までに対策を有効にすること。 ^{Δ2}</p> <p>上記以外でやむをえず ^{Δ2} 取り除けない場合には、その特権機能の目的やセキュリティ対策等をトヨタのセキュリティ主管部署に通知(*2) ^{Δ5} した上で、許可を得ること。</p> <p>ただし、車載部品非開封の特権機能がグローバルバスから、通信がなりすまされても RR6 以下の事象となるものである且つ CSP・PSP の保護対策 (VULCMN_01600 から 01900^{Δ13}) を満たす場合は、上記通知なしでの残置を許可する。 ^{Δ12}</p> <p>RR6 以下を実現する方法として、作動許可条件を用いて ECU の特権機能の作動を禁止する方法がある。</p> <p>例) ECU の特権機能の作動許可条件を車速=0km/h とする。</p> <p>ただし、作動許可条件の対象となる信号は以下の手段でなりすましから保護すること。 ^{Δ12}</p> <ul style="list-style-type: none"> - じか線、ローカル通信線、メッセージ認証 ^{Δ12} <p>*1) 特権機能を取り除くことは、特権機能のロジックの削除を指す。</p> <p>ロジックの削除ではなく、車載部品から特権機能の I/F となるコネクタを取り外すことで特権機能を使用できないようにする場合は、車載部品開封時にコネクタを復元されて、特権機能を悪用される可能性がある。このため、グローバルバスからの通信で利用できない特権機能と同様に、「4.4.1 車載部品開封の特権機能対策（テストアクセスポート）」の要件を満たす必要がある。 ^{Δ4}</p> <p>*2) 特権機能に関するトヨタのセキュリティ主管部署に通知すべき内容</p> <ul style="list-style-type: none"> - 名称 - 目的 - 用途 - 市場で機能があることによるリスク（不正使用された場合のもの） - セキュリティ対策 - セキュリティ評価仕様 - 評価結果

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		38/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

	<p>トヨタのセキュリティ主管部署には、取り除けないことが判明した時点ですみやかに通知すること。ただし、本書以外の仕様書を含めて、その特権機能に関する禁止条件が定義されていないことを、通知の前に確認すること。^{Δ5}</p> <p>例) Phase5 ダイアグ ServiceID 0xBA の禁止条件 ^{Δ5}</p>
理由	<p>セキュリティ対策をしていない特権機能が実装されている場合、他の特権機能で適切なセキュリティ処理を行っていても無意味になってしまう。</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		39/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

車載部品非開封で利用できる特権機能を悪用した攻撃を防ぐこと（出入口対策）

ID		VULCMN_00500 ^{Δ6}	
適用条件 Δ6Δ12	機能/部品	車載部品非開封で利用できる特権機能を設置する ECU ^{Δ7}	
	目標 AP ^{Δ7}	全て Δ4Δ5Δ7	
要件		<p>セキュリティ主管部署の許可を得て設置 ^{Δ4} した車載部品非開封で利用できる特権機能を悪用(*1)されないようにするために、製品出荷前に無効化するか、アクセス制御を実施すること。アクセス制御には、パスワード認証又は C&R 認証を用いること</p> <ul style="list-style-type: none">・パスワード長は 128bit 以上とすること ^{Δ6}・文字列により設定されるパスワードは少なくとも数字、大文字、小文字が含まれ、長さ 8 桁以上とすること ^{Δ9}・C&R 認証に使用する暗号鍵は 128bit 以上とすること・C&R 認証に使用する暗号アルゴリズムは、VULCMN_00100、乱数は VULCMN_00200 及び VULCMN_00300 の要件を満たすこと ^{Δ2Δ6} <p>アクセス制御について、仕様書(*4)において本書よりも詳細な対策要件が示されている場合は、それに従うこと</p> <p>*1) CSP^{Δ4}、安全、企業財産、プライバシー等の情報資産に脅威(*2)を与えること</p> <p>*2) 情報資産に対する脅威の例としては、以下がある。</p> <ul style="list-style-type: none">- CSP：CSP^{Δ4} の漏えい- 安全：リスクランク 7 以上の制御、プログラムの改ざん- 企業財産：プログラムの漏えい- プライバシー：個人・プライバシー情報(*3)の漏えい <p>*3) 個人・プライバシー情報については「車載個人・プライバシー情報対策基準書」、「車載個人・プライバシー情報対策要件書」を参照 ^{Δ5}</p> <p>*4) 「ダイアグ憲法」 ^{Δ2}、「標準リプロセキュリティ要求仕様書」等 ^{Δ1}</p>	
理由		特権機能の不正利用を防止する。	
ID	VULCMN_00501 ^{Δ6}	適用条件 Δ6Δ12	VULCMN_00500 で特権機能の無効化を採用した場合 ^{Δ7}
		機能/部品 目標 AP ^{Δ7}	全て Δ4Δ5Δ7
		車載部品非開封で利用できる特権機能を製品出荷後に使用しない場合、無効化すること	
ID	VULCMN_00502 ^{Δ6}	適用条件 Δ6Δ12	VULCMN_00500 で特権機能へのアクセス制御を採用した場合 ^{Δ7}
		機能/部品 目標 AP ^{Δ7}	10～13 ^{Δ7}

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		40/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

		車載部品非開封で利用できる特権機能を製品出荷後に使用する場合、アクセス制御を実施すること。アクセス制御には、パスワード認証又は C&R 認証を用いること。認証に使用する秘密情報（パスワード、暗号鍵）は、同一品番で共通でもよい		
ID	VULCMN_00503 ^{Δ6}	適用条件 ^{Δ6Δ12}	機能/部品	VULCMN_00500 で特権機能へのアクセス制御を採用した場合 ^{Δ7}
			目標 AP ^{Δ7}	14～20 ^{Δ7}
		<p>車載部品非開封で利用できる特権機能を製品出荷後に使用する場合、アクセス制御を実施すること。アクセス制御には、パスワード認証又は C&R 認証を用いること。認証に使用する秘密情報（パスワード、暗号鍵）は、漏えい時に他車両に影響が及ばないようにすること</p> <p>例)</p> <ul style="list-style-type: none"> ・パスワード、及び C&R 認証の暗号鍵は、各車載部品（シリアル No.毎）で個別とする。 ・公開鍵を利用する。 		

ID		VULCMN_00600 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	-
	目標 AP ^{Δ7}	-
要件		(欠番)
理由		-

ID		VULCMN_00700 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	VULCMN_00500 で特権機能へのアクセス制御を採用した場合
	目標 AP ^{Δ7}	全て ^{Δ4Δ5Δ7}
要件		<p>VULCMN_00500 の認証が通った状態（認証状態）であっても、車載部品のリセット時には認証状態が破棄され、認証が通っていない状態（未認証状態）へ移行すること</p> <p>例) 認証状態から IG-OFF ⇒ IG-ON の操作で、未認証状態に戻る</p>
理由		ディーラーにおける認証状態が維持されたままユーザに返却された場合、ユーザが特権機能を使用できる可能性がある。

車載部品非開封で利用できる特権機能を悪用した攻撃を防ぐこと(内部対策)

ID		VULCMN_00800 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	VULCMN_00500 で特権機能へのアクセス制御を採用した場合
	目標 AP ^{Δ7}	全て ^{Δ4Δ5Δ7}

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		41/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

要件	<p>VULCMN_00500 の認証後であっても、該当の特権機能にとって必要なデータのみアクセス可能であること</p> <p>(補足)</p> <p>本要件は、特権機能によってアクセスできるデータを厳密に定義することを求めるものであり、例えばダイアグ用の認証を通った後であっても、リプロ用の認証を通過していない場合は、リプロ機能が使用するデータにはアクセスできないことが求められる。</p>
理由	<p>何らかの制御パラメータを確認するための機能が暗号鍵も読出しできる場合、本来は暗号鍵を知る権利の無い者が暗号鍵を入手できてしまう。</p> <p>セキュリティの根幹に関わる暗号鍵等、重要パラメータは厳重に管理されるべきなので、読み出しはいけないものを明確にし、目的に応じたアクセス管理を徹底する必要がある。</p>

ID		VULCMN_00900 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	VULCMN_00500 で特権機能へのアクセス制御を採用した場合
	目標 AP ^{Δ7}	全て ^{Δ4Δ5Δ7}
要件	<p>VULCMN_00500 の認証前であっても、誰でもアクセスできるデータを明確化した上で、そのデータのみに対してアクセス可能であること</p> <p>(補足)</p> <p>本要件は、認証なしで誰でもアクセスできるデータを定義することを求めるものであり、例えば法規等で読出しが必要な場合、ホワイトリスト方式で必要なデータのみ読み出せるようにすることが求められる。</p>	
理由	<p>VULCMN_00800 に関連して、読出しが必要なものは明確に定義しておく必要がある。</p>	

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		42/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.3.1.2. 評価要件

ID		VULCMN_50400 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	VULCMN_00400, VULCMN_00500, VULCMN_00501, VULCMN_00502, VULCMN_00503, VULCMN_00800, VULCMN_00900 のいずれかを適用した場合 ^{Δ7}
	目標 AP ^{Δ7}	対応する対策要件の目標 AP に準ずる ^{Δ4Δ5Δ7}
要件		バックドアに繋がるデバッグ/メンテナンス機能が、トヨタと合意した範囲に制限されていることを確認すること
確認内容		バックドアの有無 メンテナンスモードの正当性

ID		VULCMN_50500 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	VULCMN_00500, VULCMN_00501, VULCMN_00502, VULCMN_00503, VULCMN_00700, VULCMN_00800, VULCMN_00900 のいずれかを適用した場合 ^{Δ7}
	目標 AP ^{Δ7}	対応する対策要件の目標 AP に準ずる ^{Δ4Δ5Δ7}
要件		対策要件が満たされていることを機能テストにより確認すること
確認内容		対策実施の有無 対策の正当性

4.3.2. 仕様面の対策

4.3.2.1. 対策要件

仕様定義段階で混入する脆弱性を利用した攻撃を防ぐこと

ID		VULCMN_01000 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	全ての ECU ^{Δ7}
	目標 AP ^{Δ7}	全て ^{Δ4Δ5Δ7}
要件		<p>トヨタ指示仕様以外の機能（隠し機能）を ECU に搭載しないこと(*)^{Δ1Δ14}</p> <p>*) 機能の無効化は含まれない。 ^{Δ14}</p> <p>既製品などで、すでにトヨタ指示仕様以外の機能（隠し機能）が搭載されている場合は、機能のロジックを削除すること。 ^{Δ14}</p> <p>やむをえず、トヨタ指示仕様以外の機能（隠し機能）を ECU に搭載する場合は、当該機能がセキュリティ要件を満足することを示し、その内容をシステム担当（各設計）、部品担当（各設計）と合意すること。 ^{Δ14}</p> <p>例）開発でのみ使用するソフトや検査ソフト等の不要なソフトは、量産品</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		43/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

	に搭載しないこと
理由	トヨタと合意していないバックドアに繋がる機能が市場製品にも残っている場合、それを活用することで本来アクセスできないデータにもアクセスする攻撃がある。余計な機能は攻撃者に利用される可能性がある。

ID		VULCMN_01100 ^{Δ6}
適用条件 Δ6Δ12	機能/部品	全ての ECU ^{Δ7}
	目標 AP ^{Δ7}	全て Δ4Δ5Δ7
要件		<p>車載部品境界の I/F (*)^{Δ4} 仕様を明確化し、</p> <ul style="list-style-type: none"> ・仕様外の入力に対して動作しないこと ・仕様外出力を出さないようにすること <p>*) 車載部品がコネクタ、無線を介して他部品と接続できる場合は、本要件の対象である ^{Δ4}</p> <p>例) ダイアグ等において、指定データ長と実際のデータ長が異なる場合等でも異常動作しないこと（例外処理を実施すること）^{Δ1}</p>
理由		異常な入力を行い、振る舞いを観測することで処理を解析する攻撃や、異常動作させて仕様外出力をさせる攻撃がある。

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		44/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.3.2.2. 評価要件

ID		VULCMN_50600 ^{Δ6}
適用条件 Δ6Δ12	機能/部品	全ての ECU ^{Δ7}
	目標 AP ^{Δ4Δ7}	全て Δ4Δ5Δ7
要件		<p>本要件は VULCMN_01000 を適用する場合に実施すること</p> <p>トヨタ指示仕様以外の機能が搭載されていないかの確認を実施すること Δ6 Δ12 Δ16</p> <p>やむをえずトヨタ指示仕様以外の機能を搭載する場合は、当該機能がセキュリティ要件を満足すること、およびその内容がトヨタと合意されていることを確認すること Δ16</p>
確認内容		<p>①トヨタ指示仕様と実装されている機能の対応関係がマトリクス表で示されているか</p> <p>②トヨタ指示仕様以外の機能が含まれていないか</p> <p>③トヨタ指示仕様以外の機能が含まれている場合、その妥当性 Δ16</p> <p>④対応関係に関するレビュー結果の一覧表が記載されているか</p>

ID		VULCMN_50700 ^{Δ6}
適用条件 Δ6Δ12	機能/部品	全ての ECU ^{Δ7}
	目標 AP ^{Δ4Δ7}	全て Δ4Δ5Δ7
要件		<p>本要件は VULCMN_01100 を適用する場合に実施すること</p> <p>対策要件が満たされていることを機能テストにより確認すること。</p>
確認内容		<p>対策実施の有無</p> <p>対策の正当性</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		45/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.3.3. セキュアコーディング

4.3.3.1. 対策要件

コーディングに起因する脆弱性を利用した攻撃を防ぐこと

ID		VULCMN_01200 ^{Δ6}										
適用条件 Δ6Δ12	機能/部品	全ての ECU ^{Δ7}										
	目標 AP ^{Δ7}	全て Δ4Δ5Δ6Δ7										
要件		<p>ソフトウェアの脆弱性を低減するため、^{Δ5} ECU に使用する全てのソフトウェアに対して以下のコーディングルールを適用すること。^{Δ16}</p> <ul style="list-style-type: none"> ・ C 言語 : TSC7030G「車載用電気電子部品組込みソフトウェアの C 言語コーディング基準」に従って、MISRA-C, CERT-C を適用すること。^{Δ13} ・ C++言語 : TSC7047G「車載用電気電子部品組込みソフトウェアの C++言語コーディング基準」に従って、MISRA-C++, AUTOSAR C++14, CERT-C++を適用すること。^{Δ13} ・ C 言語、C++言語 ^{Δ4} 以外 : 各言語に対応したセキュアコーディングルールに従うこと。 例) ISO/IEC TR 24772, CERT-JAVA, CERT-Perl <p>また、レガシーソフトウェア、モデルベース開発の自動生成コードおよび外部調達ソフトウェアについては、以下に従ってセキュアコーディング対応を行うこと。^{Δ16}</p> <table border="1"> <thead> <tr> <th>対象種別</th><th>実施内容(いずれかを実施)</th><th>対応が困難な場合</th></tr> </thead> <tbody> <tr> <td>レガシーソフトウェア</td><td rowspan="2">・ セキュアコーディングルールに従う(*1)</td><td rowspan="2">セキュリティ主管部署(本仕様書発行部署)に通知した上で合意を得る</td></tr> <tr> <td>モデルベース開発の自動生成コード</td></tr> <tr> <td>外部調達ソフトウェア</td><td>・ セキュアコーディングルールに準拠したソフトウェアを利用する ・ セキュアコーディングルールに従う(*1)</td><td>脆弱性分析を実施の上、適切なリスク対応(保有/回避/共有/低減)を行う</td></tr> </tbody> </table> <p>*1)セキュアコーディングチェックが可能な静的コード解析ツールで確認(*2)^{Δ5}を行い、セキュリティ上許容(*3)できない場合は ^{Δ5} 対策を行う方法でもよい。^{Δ16}</p> <p>*2) ソフトウェアベンダから確認結果を受け取って確認しても良い</p> <p>*3) CSP、安全、企業財産、プライバシーなどの情報資産に脅威(*4)を与えないことを確認 ^{Δ5}</p> <p>*4) 情報資産に対する脅威の例としては、以下がある。^{Δ5}</p>	対象種別	実施内容(いずれかを実施)	対応が困難な場合	レガシーソフトウェア	・ セキュアコーディングルールに従う(*1)	セキュリティ主管部署(本仕様書発行部署)に通知した上で合意を得る	モデルベース開発の自動生成コード	外部調達ソフトウェア	・ セキュアコーディングルールに準拠したソフトウェアを利用する ・ セキュアコーディングルールに従う(*1)	脆弱性分析を実施の上、適切なリスク対応(保有/回避/共有/低減)を行う
対象種別	実施内容(いずれかを実施)	対応が困難な場合										
レガシーソフトウェア	・ セキュアコーディングルールに従う(*1)	セキュリティ主管部署(本仕様書発行部署)に通知した上で合意を得る										
モデルベース開発の自動生成コード												
外部調達ソフトウェア	・ セキュアコーディングルールに準拠したソフトウェアを利用する ・ セキュアコーディングルールに従う(*1)	脆弱性分析を実施の上、適切なリスク対応(保有/回避/共有/低減)を行う										

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		46/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

	<ul style="list-style-type: none"> - CSP : CSP の漏えい ^{Δ5} - 安全 : リスクランク 7 以上の制御、プログラムの改ざん ^{Δ5} - 企業財産 : プログラムの漏えい ^{Δ5} - プライバシー : 個人・プライバシー情報(*5)の漏えい ^{Δ5} <p>*5) 個人・プライバシー情報については「車載個人・プライバシー情報対策基準書」、「車載個人・プライバシー情報対策要件書」を参照 ^{Δ5}</p> <p>対策の要否については、システム担当（各設計）、部品担当（各設計）、コーディング主管部署（PQF^{Δ5}）、セキュリティ主管部署（本仕様書発行部署）とサプライヤで協議を行なうこと。</p>
理由	ルールに従いコーディングを行うことで、脆弱性の低減を行なう。

プログラムを解析されることを防ぐこと（PCB 上の ROM、マイコン内プログラム）

ID		VULCMN_01300 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	全ての ECU ^{Δ7}
	目標 AP ^{Δ7}	全て ^{Δ4Δ6Δ7}
要件		<p>車載部品の PCB 上の ROM やマイコン内の Flash にシンボル一覧を書き込まないこと（試作時は除く）</p> <p>※プログラミング言語が C, C++の場合</p>
理由		<p>シンボル一覧が市場でも車載部品に残存する場合、それが解析され、悪用(*)されないようにするために、シンボル一覧を残さないようにする必要がある。^{Δ7}</p> <p>*) VULCMN_00500 の(*1)を参照。</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		47/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.3.3.2. 評価要件

ID		VULCMN_50800 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	全ての ECU ^{Δ7}
	目標 AP ^{Δ4Δ7}	全て ^{Δ4Δ5Δ7}
要件		<p>ソフトウェアが VULCMN_01200 に記載の各プログラミング言語に応じたコーディングルールに準拠していることを確認すること。^{Δ16}</p> <p>レガシーソフトウェアおよび自動生成コードについては、セキュアコーディングルールに準拠していることを確認すること。</p> <p>セキュアコーディングルールの準拠確認に静的コード解析ツールを用いる場合には、「推奨ツール」を参考にすること。</p> <p>また、静的コード解析ツールで確認ができない項目については、対策要件が満たされていることをソースコードレビューにより確認すること。^{Δ16}</p> <p>外部調達ソフトウェアについては、セキュアコーディング対応していることを確認すること。セキュアコーディング対応をしていない場合、リスク対応ができていないことを確認すること。^{Δ16}</p> <p>ルールに違反している箇所がある場合、違反している理由がセキュリティ上許容できるものであること ^{Δ12}</p>
推奨ツール		Klocwork, Coverity, CodeSonar, QA・C, LDRA, Fortify SCA (最新バージョンのツールの使用を推奨)
確認内容		実装上の脆弱性の有無

ID		VULCMN_50900 ^{Δ6Δ16}
適用条件 ^{Δ6Δ12}	機能/部品	-
	目標 AP ^{Δ7}	-
要件		(欠番)
確認内容		

ID		VULCMN_51000 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	全ての ECU ^{Δ7}
	目標 AP ^{Δ7}	全て ^{Δ4Δ6Δ7}
要件		本要件は VULCMN_01300 を適用する場合に実施すること ダンプした書込み用バイナリにシンボルが含まれていないこと

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		48/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

確認内容	書込み用バイナリにシンボル記号が含まれていないか
------	--------------------------

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		49/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.3.4. プログラム／データの保護対策（プログラムの保護）

4.3.4.1. 対策要件

プログラムを改ざんされる攻撃を防ぐこと（マイコン内プログラム）

ID		VULCMN_01400 ^{Δ6}
適用条件 Δ6 ^{Δ12}	機能/部品	リプログラミング機能を持つ ECU
	目標 AP ^{Δ7}	全て Δ4 ^{Δ5} Δ7
要件		車載部品外部から受信したプログラムは完全性を確認してから実行すること 例）リプログラミング時は、受信したプログラムの完全性を確認してフラグを格納し、次回ブート時にはフラグのチェックのみを行う
理由		リプログラミング機能を持つ車載部品は、プログラム書き換え時に正当なプログラムであることを確認し、不正なプログラムで動作することを防止する必要がある。リプログラミング機能搭載車載部品は確実に対応する必要がある。

ID		VULCMN_01500 ^{Δ6} Δ12
適用条件 Δ6 ^{Δ12}	機能/部品	
	目標 AP ^{Δ7}	
要件		（欠番）
理由		

4.3.4.2. 評価要件

ID		VULCMN_51100 ^{Δ6}
適用条件 Δ6 ^{Δ12}	機能/部品	VULCMN_01400 を適用した場合 Δ7 ^{Δ12}
	目標 AP ^{Δ7}	対応する対策要件の目標 AP に準ずる Δ4 ^{Δ5} Δ7
要件		対策要件が満たされていることを機能テストにより確認すること
確認内容		対策実施の有無 対策の正当性

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		50/66
Application: In-vehicle parts in which cyber security countermeasure are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

4.3.5. プログラム／データの保護対策（CSP・PSPの保護）

4.3.5.1. 対策要件

CSPを漏えい、改ざんされる攻撃を防ぐこと/PSPを改ざんされる攻撃を防ぐこと

ID		VULCMN_01600 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	パスワードを使用・格納する ECU ^{Δ7}
	目標 AP ^{Δ7}	全て ^{Δ4Δ5Δ7}
要件		<p>以下の①もしくは②の要件を満たすこと ^{Δ13}</p> <p>①パスワードについて、VULCMN_01700, VULCMN_01701, VULCMN_01702 の CSP の保護要件を満たすこと。 ^{Δ13}</p> <p>②パスワードについて、メモリにハッシュ値に変換して格納すること。 ハッシュ値に変換したパスワードは PSP であるため、VULCMN_01700, VULCMN_01701, VULCMN_01702 の PSP の保護要件を満たすこと。 ^{Δ13}</p>
理由		パスワードが仮に読み出されたとしても、利用できない形で格納する必要がある。

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		51/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

ID		VULCMN_01700 ^{Δ6}		
適用条件 Δ6Δ12	機能/部品	CSP・PSP を格納する ECU ^{Δ7}		
	目標 AP ^{Δ7}	全て Δ4Δ5 ^{Δ7}		
要件		CSP はセキュアなメモリ(*)に格納すること *) セキュアなメモリ - 外部からのアクセス(Read/Write)を制限されたメモリ - 特定のタスクのみアクセスできるメモリ Δ13 - HSM 内部の演算装置のみが直接アクセスできるメモリ Δ13 保護対象データが PSP の場合は、Write が制限されたメモリに格納すること (Read は制限されなくてもよく、HSM 内部の演算装置のみが直接アクセスできるメモリ Δ13 への格納は必須ではない) ^{Δ7}		
理由		最低限、外部（ダイアグ等の特権機能及び JTAG 等のマイコンレベルの特権機能）からのアクセス(Read/Write)を制限されたメモリに CSP を格納する必要がある(PSP の場合は Write の制限)。 ^{Δ7} ソフトウェアを乗っ取る等、より高度な攻撃を警戒する場合は CPU からのアクセスも制限する必要がある。		
ID	VULCMN_01701 ^{Δ6}	適用条件	機能/部品	CSP・PSP を格納する ECU ^{Δ4Δ5Δ7}
		Δ6Δ12	目標 AP ^{Δ7}	全て Δ4Δ5 ^{Δ7}
		CSP をマイコン内のメモリに格納する場合、外部から直接読み書きできないように、外部からのアクセス(Read/Write)を制限すること。 特定の関数のみが読出し・書き込みを行う設計とすること。 PSP をマイコン内のメモリに格納する場合、外部からの Write を制限すること。 ^{Δ14} (Read は制限しなくてもよい) ^{Δ7} やむをえず、CSP をマイコン外付けメモリに格納する場合、暗号化、且つ、改ざん検知（署名検証） ^{Δ4} を実施すること。 ^{Δ2} やむを得ず PSP をマイコン外付けメモリに格納する場合、改ざん検知を実施すること。 ^{Δ14} (暗号化は実施しなくてもよい) ^{Δ7} - AP10～13 ^{Δ7} ：暗号化、改ざん検知に使用する暗号鍵は、同一品番で共通でもよい。 ^{Δ2} - AP14～20 ^{Δ7} ：暗号化、改ざん検知に使用する暗号鍵は、漏えい時に他車両に影響が及ばないようにすること。 ^{Δ2} 上記の暗号化または改ざん検知に使用した暗号鍵の保護は VULCMN_01702 の要件を満たすこと。 ^{Δ10Δ13}		

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		52/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

		例) $\Delta 2$ ・暗号鍵は、各車載部品（シリアル No.毎）で個別とする。 $\Delta 2$ ・公開鍵を利用する。 $\Delta 2$		
ID	VULCMN_01702 $\Delta 1\Delta 6$	適用条件	機能/部品	CSP・PSP を格納する ECU $\Delta 7\Delta 10$
		$\Delta 6\Delta 12$	目標 AP $\Delta 7$	14~20 $\Delta 4\Delta 5\Delta 7\Delta 10$
		HSM $\Delta 13$ を搭載し $\Delta 10$ 、HSM 内部の演算装置 $\Delta 13$ のみが直接 CSP・PSP $\Delta 14$ にアクセスできるようにすること ただし、CSP の生成、更新、使用の処理を目的としたセッションキーは本要件の対象外とし、VULCMN_01701 を満たすこと。その場合、処理終了後すぐに CSP を当該メモリから消去すること $\Delta 13$ 消去の例) 当該メモリの CSP をゼロで上書き $\Delta 13$ やむをえず、PSP をマイコン内のメモリに格納する場合はハードウェア機能を用いて外部からの Write を制限すること $\Delta 14$ やむをえず、PSP をマイコン外付けメモリに格納する場合は、改ざん検知可能な状態(MAC もしくは署名を付与した状態)で格納すること $\Delta 7$ 。また、改ざん検知に使用する暗号鍵は HSM 内部の演算装置のみが直接アクセスできるようにすること $\Delta 14$		

ID		VULCMN_01800 $\Delta 6$
適用条件 $\Delta 6\Delta 12$	機能/部品	CSP・PSP を配布する ECU $\Delta 7$
	目標 AP $\Delta 7$	全て $\Delta 4\Delta 5\Delta 7$
要件		CSP を他の車載部品へ配布する場合、機密性、完全性を保ったまま配布すること 保護対象データが PSP の場合は、完全性を保ったまま配布すること (機密性は確保しなくてもよい) $\Delta 7$ 例) 鍵共有プロトコルの活用、知識分散等
理由		CSP・PSP を配布する場合、CSP $\Delta 4$ が漏えい・改ざん(PSP の場合は改ざん)されないように、暗号化や MAC 等により機密性・完全性を保つ必要がある。

ID		VULCMN_01900 $\Delta 6$
適用条件 $\Delta 6\Delta 12$	機能/部品	CSP・PSP を格納する ECU $\Delta 7$
	目標 AP $\Delta 7$	全て $\Delta 4\Delta 5\Delta 7$
要件		電源断等で CSP・PSP $\Delta 7$ の更新処理が途中で途絶えた場合、更新前の状態を維持すること

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		53/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

理由	更新が中断した場合、CSP・PSP がデタラメな値になるとセキュリティ機能そのものが意味を成さなくなるため、更新前の値に戻る必要がある。
----	--

ID		VULCMN_02000 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	
	目標 AP ^{Δ7}	
要件		(欠番) ^{Δ13}
理由		

4.3.5.2. 評価要件

ID		VULCMN_51200 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	VULCMN_01600,VULCMN_01700, VULCMN_01701, VULCMN_01702, VULCMN_01800, VULCMN_01900 のいずれかを適用した場合 ^{Δ7}
	目標 AP ^{Δ7}	対応する対策要件の目標 AP に準ずる ^{Δ4Δ5Δ7}
要件		対策要件が満たされていることを機能テストにより確認すること
確認内容		対策実施の有無 対策の正当性

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		54/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.3.6. プログラム／データの保護対策（情報系車載部品のデータの保護）

4.3.6.1. 対策要件

情報系データを漏えい、改ざんされる攻撃を防ぐこと

ID		VULCMN_02100 ^{Δ6}
適用条件 Δ6Δ12	機能/部品	TCP、又は UDP ポートを持つ ECU ^{Δ7}
	目標 AP ^{Δ7}	全て Δ4Δ5Δ7
要件 Δ14		<ul style="list-style-type: none"> ・ エントリーポイントの TCP、又は UDP ポートの場合、使用しない TCP/UDP ポートは閉じておくこと。使用する TCP/UDP ポートはサービス開始時・コネクション確立要求時に開け、サービス終了時・コネクション終了時に閉じること。 ・ エントリーポイント以外の TCP、又は UDP ポートの場合、使用しない TCP/UDP ポートは閉じておくこと。
理由		不要なポートが開いていると外部からの攻撃に悪用される危険性がある。

ID		VULCMN_02200 ^{Δ6}
適用条件 Δ6Δ12	機能/部品	ファイルシステムを持つ OS を使用する ECU ^{Δ7}
	目標 AP ^{Δ7}	全て Δ4Δ5Δ7
要件		<p>各ファイルやディレクトリに対して、デフォルトのアクセス権の設定（パーミッション）は Read only とすること</p> <p>読み取り以外（書き換え・実行等）が必要な場合は、その対象のファイルやディレクトリ、それが可能な対象ユーザ（所有者/所有グループに属するユーザ/その他のユーザ/全てのユーザ等）を明確化すること</p>
理由		ファイルやディレクトリのアクセス権は、最小限である必要がある。

ID		VULCMN_02300 ^{Δ6}
適用条件 Δ6Δ12	機能/部品	複数の CPU モードを利用できる ECU ^{Δ7}
	目標 AP ^{Δ7}	全て Δ4Δ5Δ7
要件		特権モード、ユーザモードを厳密に分けて定義し、各モードでどのデータにアクセス可能か明確化すること
理由		OS/OSS の機能も活用して、データのアクセス権管理を行う必要がある。

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		55/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

ID		VULCMN_02400 ^{△6△12}
適用条件 △6△12	機能/部品	
	目標 AP ^{△8}	
要件		(欠番)
理由		

ID		VULCMN_03700 ^{△9△10}
適用条件 ^{△12}	機能/部品	3rdParty アプリ(*1)またはセキュリティ要求が満足できないアプリ(*2) △10 を搭載する機能を持つ ECU *1) トヨタが開発に関与しないアプリ。ここで関与しないとはトヨタとの開発契約に基づかないことを指す。△10 *2)引き当てられたセキュリティ要求が満足できないことをシステム担当（各設計）、部品担当（各設計）、セキュリティ主管部署（本仕様書発行部署）と合意したアプリ。△10
	目標 AP	14~20
要件		3rdParty アプリまたはセキュリティ要求が満足できないアプリ △10 が配置されるエントリーポイント領域は以下を満たすこと ・3rdParty アプリまたはセキュリティ要求が満足できないアプリ △10 から出力されるデータは、リスクランク 7 以上の制御に影響しないようにすること ・OS が 3rdParty アプリまたはセキュリティ要求が満足できないアプリ △10 に対し付与するデータ/機能へのアクセス権 (Read/Write/Execute)はユーザが許可したものに限定すること
理由		意図せずマルウェアをインストールされ、実行された場合のリスクを最小限に抑えるため。

ID		VULCMN_03800 ^{△9}
適用条件 ^{△12}	機能/部品	ログイン機能を持つ OS を使用する ECU
	目標 AP	全て
要件		root ユーザの直接ログインを禁止し、かつ一般ユーザの権限昇格操作を制限すること
理由		root ユーザは特権的な権限である。システム悪用のリスクが高いため、個別の必要最小権限を付与したユーザで動作することが必要である。

ID		VULCMN_03900 ^{△10}
----	--	-----------------------------

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		56/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

適用条件 $\Delta 12$	機能/部品	ログイン機能を持つ OS を使用する ECU
	目標 AP	全て
要件		OS にログインするために設定されるパスワードは少なくとも数字、大文字、小文字が含まれ、長さ 8 桁以上にすること
理由		安全性の低いパスワードが設定されることで、ブルートフォースアタック等により不正にログインされてしまう可能性がある。

ID		VULCMN_04000 $\Delta 10$
適用条件 $\Delta 12$	機能/部品	パスワード認証機能を持つアプリ
	目標 AP	全て
要件		アプリで使用されるパスワードは少なくとも数字、大文字、小文字が含まれ、長さ 8 桁以上とするか、もしくは上記条件を満たせないパスワードが設定される場合、お客様にリスクを提示すること
理由		安全性の低いパスワードが設定されることで、ブルートフォースアタック等によりアプリを不正利用される可能性がある。十分な強度のパスワードの設定が困難な場合は、お客様へ注意を提示することで適切な利用を促す。

4.3.6.2. 評価要件

ID		VULCMN_51300 $\Delta 6$
適用条件 $\Delta 12$	機能/部品	TCP、又は UDP ポートを持つ ECU
	目標 AP $\Delta 7$	全て $\Delta 7$
要件		本要件は VULCMN_02100 を適用する場合に実施すること 対策要件が満たされていることを設計検証により確認すること。
確認内容		<p>対策の正当性</p> <p>対策の正当性については、下記の項目を確認すること。</p> <p><対策の正当性の確認項目></p> <ul style="list-style-type: none"> - 開きポートに対応する仕様の名称 - ポート番号 - サービス名称 - 概要 - 目的 - 用途 - ポートが開いているときのセキュリティ対策実施の有無

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		57/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

	<ul style="list-style-type: none"> - ポート・サービスがある場合のリスク(不正使用された場合のもの) - セキュリティ対策 - セキュリティ評価仕様 - 評価結果
--	---

ID		VULCMN_51400 ^{Δ6}
適用条件 Δ6Δ12	機能/部品	VULCMN_02200, VULCMN_02300 のいずれかを適用した場合 ^{Δ7}
	目標 AP ^{Δ7}	全て ^{Δ4Δ5Δ7}
要件		対策要件が満たされていることを OS/OSS の ^{Δ1} 環境設定から確認すること
確認内容		<p>対策の正当性</p> <p>対策の正当性については、下記の項目を確認すること。</p> <p><対策の正当性の確認項目></p> <ul style="list-style-type: none"> - ファイルやディレクトリの名称 - 概要 - 目的 - 用途 - 対策実施の有無 - そのアクセス権、対象ユーザである場合のリスク - そのセキュリティ対策 - セキュリティ評価仕様 - 評価結果

ID		VULCMN_51500 ^{Δ6Δ12}
適用条件 ^{Δ12}	機能/部品	
	目標 AP ^{Δ8}	
要件		(欠番)
確認内容		

ID		VULCMN_52600 ^{Δ9}
適用条件 ^{Δ12}	機能/部品	3rdParty アプリまたはセキュリティ要求が満足できないアプリ ^{Δ10} を搭載する機能を持つ ECU
	目標 AP	14~20
要件		<p>本要件は VULCMN_03700 を適用する場合に実施すること</p> <p>対策要件が満たされていることを設計検証により確認すること</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		58/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

確認内容	対策実施の有無 対策の正当性
------	-------------------

ID		VULCMN_52700 ^{Δ9}
適用条件 ^{Δ12}	機能/部品	ログイン機能を持つ OS を使用する ECU
	目標 AP	全て
要件		本要件は VULCMN_03800 を適用する場合に実施すること 対策要件が満たされていることを機能テストにより確認すること
確認内容		対策実施の有無 対策の正当性

ID		VULCMN_52800 ^{Δ10}
適用条件 ^{Δ12}	機能/部品	ログイン機能を持つ OS を使用する ECU
	目標 AP	全て
要件		本要件は VULCMN_03900 を適用する場合に実施すること 対策要件が満たされていることを機能テストにより確認すること
確認内容		対策実施の有無 対策の正当性

ID		VULCMN_52900 ^{Δ10}
適用条件 ^{Δ12}	機能/部品	パスワード認証機能を持つアプリ
	目標 AP	全て
要件		本要件は VULCMN_04000 を適用する場合に実施すること 対策要件が満たされていることを機能テストにより確認すること
確認内容		対策実施の有無 対策の正当性

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		59/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.4. 車載部品開封攻撃への耐性

車載部品を開封したうえで、物理的にアクセスして解析・改ざんする攻撃への対策を示す。

4.4.1. 車載部品開封の特権機能対策（テストアクセスポート）

4.4.1.1. 対策要件

車載部品を開封して利用できる特権機能を悪用した攻撃を防ぐこと

ID		VULCMN_02500 ^{Δ6}		
適用条件 Δ6 ^{Δ12}	機能/部品	車載部品を開封して利用できる特権機能を設置する ECU ^{Δ7}		
	目標 AP ^{Δ7}	全て Δ4 ^{Δ5} Δ7		
要件		<p>車載部品を開封して利用できる特権機能（テストアクセスポート）を悪用されないようにするために、製品出荷前に無効化するか、アクセス制御を実施すること。</p> <p>アクセス制御には、パスワード認証又は C&R 認証を用いること。</p> <ul style="list-style-type: none">・パスワード長は 128bit 以上とすること Δ6・文字列により設定されるパスワードは少なくとも数字、大文字、小文字が含まれ、長さ 8 桁以上にすること・C&R 認証に使用する暗号鍵は 128bit 以上とすること・C&R 認証に使用する暗号アルゴリズムは、VULCMN_00100、乱数は VULCMN_00200 及び VULCMN_00300 の要件を満たすこと Δ2^{Δ6} <p>対策実施時期：遅くとも 1A の製品出荷前までに対策を有効にすること。Δ2</p>		
理由		特権機能使用時、認証を行うことで不正利用を防止する必要がある。		
ID	VULCMN_02501	適用条件 Δ6 ^{Δ12}	機能/部品	VULCMN_02500 で特権機能の無効化を採用した場合 Δ7
			目標 AP ^{Δ7}	全て Δ4 ^{Δ5} Δ7
		車載部品を開封して利用できる特権機能を製品出荷後に使用しない場合、無効化すること。		
ID	VULCMN_02502	適用条件 Δ6 ^{Δ12}	機能/部品	VULCMN_02500 で特権機能へのアクセス制限を採用した場合 Δ7
			目標 AP ^{Δ7}	10～13 ^{Δ4} Δ7
		車載部品を開封して利用できる特権機能を製品出荷後に Δ4 使用する場合、アクセス制御を実施すること。アクセス制御には、パスワード認証又は C&R 認証を用いること。認証に使用する秘密情報（パスワード、暗号鍵）は、同一品番で共通でもよい。		
ID	VULCMN_02503	適用条件	機能/部品	VULCMN_02500 で特権機能へのアクセス制限を採用し

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		60/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

		Δ6Δ12		た場合 Δ7
			目標 APΔ7	14～20Δ4Δ5Δ7
		<p>車載部品を開封して利用できる特権機能を製品出荷後に Δ4 使用する場合、アクセス制御を実施すること。アクセス制御には、パスワード認証又は C&R 認証を用いること。認証に使用する秘密情報（パスワード、暗号鍵）は、漏えい時に他車両に影響が及ばないようにすること。</p> <p>例)</p> <ul style="list-style-type: none"> ・パスワード、及び C&R 認証の暗号鍵は、各車載部品（シリアル No.毎）で個別とする。 ・公開鍵を利用する。 		

ID		VULCMN_02600 ^{Δ6}		
適用条件 Δ6Δ12	機能/部品	VULCMN_02500 で特権機能へのアクセス制御を採用した場合 ^{Δ7}		
	目標 AP ^{Δ7}	全て ^{Δ4Δ5Δ7}		
要件		車載部品を開封して利用できる特権機能から、保護されたメモリ、CSP を読み取ることができないこと VULCMN_02601、及び VULCMN_02602 の対策を実施すること ^{Δ7}		
理由		不良解析時であっても、暗号鍵等の読出しができないようにした方がセキュアなため。暗号化の結果による確認等の間接的な確認が必要になる。		
ID	VULCMN_02601 ^{Δ7}	適用条件 Δ12	機能/部品	メモリのアクセス権管理機能を利用できる場合
			目標 AP	全て
		メモリのアクセス権管理機能により、特権機能から保護されたメモリ、CSP への Read を禁止すること		
ID	VULCMN_02602 ^{Δ7}	適用条件 Δ12	機能/部品	全ての ECU
			目標 AP	14～20
		車載部品を開封して利用できる特権機能からバスが分離されたセキュア領域に CSP を格納し、HSM 内部の演算装置 ^{Δ13} のみが CSP にアクセスできるようにすること		

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		61/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.4.1.2. 評価要件

ID		VULCMN_51600 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	VULCMN_02500, VULCMN_02501, VULCMN_02502, VULCMN_02503, VULCMN_02600 のいずれかを適用した場合 ^{Δ7}
	目標 AP ^{Δ7}	対応する対策要件の目標 AP に準ずる ^{Δ4Δ5Δ7}
要件		対策要件が満たされていることを機能テストにより確認すること
確認内容		対策実施の有無 対策の正当性

ID		VULCMN_51700 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	VULCMN_02500, VULCMN_02501, VULCMN_02502, VULCMN_02503, VULCMN_02600 のいずれかを適用した場合 ^{Δ7}
	目標 AP ^{Δ4Δ7}	対応する対策要件の目標 AP に準ずる ^{Δ4Δ5Δ7}
要件		バックドアに繋がるデバッグ/メンテナンス機能で利用できる範囲が、リスクのない範囲に制限されていることを確認すること
確認内容		バックドアの有無 メンテナンスモードの正当性

4.4.2. PCB 解析対策

4.4.2.1. 対策要件

チップ間でやりとりされる機密情報の解析を防ぐこと

ID		VULCMN_02700 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	車載部品上のマイコン間、マイコンと外部メモリで通信する ECU ^{Δ7}
	目標 AP ^{Δ7}	全て ^{Δ4Δ5Δ7}
要件		車載部品上のマイコン間、マイコンと外部メモリ間の通信に CSP が含まれる場合、その暗号化により解析を防ぐこと（AP14 以上は、セキュアマイコンに上述の機密情報が保管されること）
理由		設計上の理由により、マイコン間、マイコンと外部メモリ間で CSP をやり取りする必要がある場合には、それらを解析できないようにする必要がある。

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		62/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

ID		VULCMN_02800 ^{Δ6}
適用条件 Δ6Δ12	機能/部品	車載部品上のマイコン間、マイコンと外部メモリで通信する ECU ^{Δ7}
	目標 AP ^{Δ7}	20 ^{Δ4Δ5Δ7}
要件		車載部品上のマイコンとセキュリティチップ間の通信の暗号化により機密情報の解析を防ぐこと
理由		設計上の理由により、マイコンとセキュリティチップ間で機密情報をやり取りする必要がある場合には、機密情報を解析できないようにする必要がある。

4.4.2.2. 評価要件

ID		VULCMN_51800 ^{Δ6}
適用条件 Δ12	機能/部品	車載部品上のマイコン間、マイコンと外部メモリで通信する ECU ^{Δ7}
	目標 AP ^{Δ7}	全て Δ7
要件		本要件は VULCMN_02700 を適用する場合に実施すること 対策要件が満たされていることを設計検証により確認すること
確認内容		対策実施の有無 対策の正当性

ID		VULCMN_51900 ^{Δ6}
適用条件 Δ12	機能/部品	車載部品上のマイコン間、マイコンと外部メモリで通信する ECU ^{Δ7}
	目標 AP ^{Δ7}	20 ^{Δ7}
要件		本要件は VULCMN_02800 を適用する場合に実施すること 対策要件が満たされていることを設計検証により確認すること
確認内容		対策実施の有無 対策の正当性

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		63/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.4.3. 耐タンパ

4.4.3.1. 対策要件

物理的な解析や攻撃を防ぐこと

ID		VULCMN_02900 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	センターから認証を要求される ECU ^{Δ7Δ16}
	目標 AP ^{Δ7}	20 ^{Δ4Δ5Δ7}
要件		センター ^{Δ16} からの認証に用いられる CSP(*)について ^{Δ8} 、電磁波による解析に耐性をもつこと *)クライアント認証用の鍵情報(共通鍵、秘密鍵)等 ^{Δ8}
理由		サイドチャネル攻撃によりチップ内の CSP が解析されることを防ぐため。

ID		VULCMN_03000 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	センターから認証を要求される ECU ^{Δ7Δ16}
	目標 AP ^{Δ7}	20 ^{Δ4Δ5Δ7}
要件		センター ^{Δ16} からの認証に用いられる CSP(*)について ^{Δ8} 、電流を測定する解析に耐性をもつこと *)クライアント認証用の鍵情報(共通鍵、秘密鍵)等 ^{Δ8}
理由		サイドチャネル攻撃によりチップ内の CSP が解析されることを防ぐため。

ID		VULCMN_03100 ^{Δ6Δ12}
適用条件 ^{Δ6Δ12}	機能/部品	
	目標 AP ^{Δ7}	
要件		(欠番)
理由		

ID		VULCMN_03200 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	センターから認証を要求される ECU ^{Δ7Δ16}
	目標 AP ^{Δ7}	20 ^{Δ4Δ5Δ7}
要件		電圧センサを搭載すること
理由		サイドチャネル攻撃によりチップ内のセンターからの認証に用いられる ^{Δ16} CSP が解析されることを検知するため。この検知信号を受けて更なる解析がされない又は安全停止できるようにセキュリティ機能を切り替えるため。

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		64/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

ID		VULCMN_03300 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	センターから認証を要求される ECU ^{Δ7Δ16}
	目標 AP ^{Δ7}	20 ^{Δ4Δ5Δ7}
要件		周波数センサを搭載すること
理由		サイドチャネル攻撃によりチップ内のセンターからの認証に用いられる ^{Δ16} CSP が解析されることを検知するため。この検知信号を受けて更なる解析がされない又は安全停止できるようにセキュリティ機能を切り替えるため。

ID		VULCMN_03400 ^{Δ6}
適用条件 ^{Δ12}	機能/部品	VULCMN_00500 で特権機能へのアクセス制御を採用した場合、又は VULCMN_02500 で特権機能へのアクセス制御を採用した場合 ^{Δ7}
	目標 AP ^{Δ7}	20 ^{Δ7}
要件		特権機能へのアクセス制御に対する認証回避、認証誤判定につながる電源グリッチ ^{Δ7} 攻撃への対策(*)を実施すること *)対策例として、特権機能へのアクセス制御の認証判定を複数回行う等がある ^{Δ8}
理由		認証回避、認証誤判定による、特権機能 ^{Δ7} からのソフト不正書換え等を防ぐため。

ID		VULCMN_03500 ^{Δ6}
適用条件 ^{Δ12}	機能/部品	センターから認証を要求される ECU ^{Δ7Δ16}
	目標 AP ^{Δ7}	20 ^{Δ7}
要件		センター ^{Δ16} からの認証に用いられる CSP(*1)について ^{Δ8} 、タイミング解析に耐性をもつこと(*2) *1)クライアント認証用の鍵情報(共通鍵、秘密鍵)等 ^{Δ8} *2)対策例として、CSP を扱う演算の時間平滑化やランダム化等がある ^{Δ8}
理由		サイドチャネル攻撃によりチップ内の CSPが解析されることを防ぐため。

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		65/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.4.3.2. 評価要件

ID		VULCMN_52000 ^{Δ6}
適用条件 ^{Δ12}	機能/部品	VULCMN_02900, VULCMN_03000, VULCMN_03400, VULCMN_03500 のいずれかを適用した場合 ^{Δ7}
	目標 AP ^{Δ7}	対応する対策要件の目標 AP に準ずる ^{Δ7}
要件		対策要件が満たされていることを設計検証により確認すること
確認内容		対策実施の有無 対策の正当性

ID		VULCMN_52100 ^{Δ6Δ12}
適用条件 ^{Δ12}	機能/部品	
	目標 AP ^{Δ7}	
要件		(欠番)
確認内容		

ID		VULCMN_52200 ^{Δ6}
適用条件 ^{Δ6Δ12}	機能/部品	VULCMN_03200, VULCMN_03300 のいずれかを適用した場合 ^{Δ7}
	目標 AP ^{Δ7}	対応する対策要件の目標 AP に準ずる ^{Δ7}
要件		対策要件が満たされていることを機能テストにより確認すること
確認内容		対策実施の有無 対策の正当性

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		66/66
Application: In-vehicle parts in which cyber security countermeasure are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

5. (欠番) Δ6 Δ15

5.1. (欠番) Δ6 Δ15

ID		VULCMN_52300
適用条件 Δ12	機能/部品	-
	目標 APΔ7	-
要件		(欠番)
理由		-
参考要件		-

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		1/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

Change History^{A1}

Mark	Ver.	Date	Revised by	Item	Description
	1.0	Aug.12, 2016	51F Sawada	All items	First version issued.
Δ1	1.1	Oct.28, 2016	51F Sawada	3.2.2.2	Clarification of Evaluation Requirements (SPC-0001). It's described on table.
↑	↑	↑	↑	3.2.3.2	Clarification of Evaluation Requirements (SCD-0002). It's described on table.
↑	↑	↑	↑	1.6	Format to describe list of the related document is changed from bullet points form to tabular one (Table 1.3, Table 1.4).
↑	↑	↑	↑	2.2	Name of evaluation method is changed.
↑	↑	↑	↑	All items	Error correction of the others.
Δ2	1.2	Apr.24, 2017	51F Sawada	3.2.1.1	Clarification of the due date for Countermeasure Requirements (PRV-0001). Clarification of the acceptable case to remain the Privileged Functions of In-vehicle Parts without Opening.
↑	↑	↑	↑	3.2.5.1	Addition of the countermeasure of the case to store the password in the external memory of the microcontroller to Countermeasure Requirements (CSP-0001).
↑	↑	↑	↑	3.2.5.1	Addition of the countermeasure of the case to store the CSP in the external memory of the microcontroller to Countermeasure Requirements (CSP-0002).
↑	↑	↑	↑	3.3.1.1	Clarification of the due date for Countermeasure Requirements (TAC-0001).
↑	↑	↑	↑	All items	Error correction of the others.
Δ3	1.3	Sep.29, 2017	51F Sawada	1.6	The requirements title on the list of related documents changed. (Requirements Specification of CCP/XCP changed to CCP/XCP Security Requirements.)
↑	↑	↑	↑	3	Sort order of each requirement of Vulnerability Countermeasure and Vulnerability Countermeasure incorporation Check changed.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		2/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

↑	↑	↑	↑	3.1.2	Entropy requirement of random number for L2, L3 ECU changed to the value for each random number use case.
↑	↑	↑	↑	All items	Error correction of the others.
Δ4	1.4	Apr.25, 2018	51F Sawada	1.5	Clarification of CSP (Table 1.1)
↑	↑	↑	↑	2.1	Clarification of Exploitation of privileged functions of in-vehicle parts without opening (Table 2.1)
↑	↑	↑	↑	3	Clarification of terms and applicable security levels, addition of evaluation requirement (ID) to contents of evidence, clarification of documentation of Requirement Incorporation Check Judgment Criteria and Evaluation Check Judgment Criteria
↑	↑	↑	↑	All items	Error correction of the others.
Δ5	1.5	Dec.13, 2018	51F Ozaki	Top page	Addition of special note.
↑	↑	↑	↑	1.6	Deletion of related documents not referred in this document. Addition of specification numbers. Addition of "Abbreviation in this document" to Table 1.4.
↑	↑	↑	51F Sawada	1.8	Addition of submitting way of check list and evidence
↑	↑	↑	51F Ozaki	3.1.2.1	Addition of a comment on how to use the true random number generator. Algorithm unpredictability requirement of random number changed to the value for each random number use case.
↑	↑	↑	↑	3.2.1.1	Addition of notice time. Addition of annotation about prohibition condition.
↑	↑	↑	51F Sawada	3.2.3.1	Clarification of that deviation procedure shall perform MISRA Compliance. Clarification of that judgment criteria for permissible in terms of security is that there shall not be concern of non-compliance described in explanation of secure coding rule which is corresponded to each

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		3/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

					language about external procurement software and legacy software Symbol code for the department in charge of the coding is changed to PQF.
↑	↑	↑	↑	All items	Deletion of security level L4. Deletion of description as “to be submitted” about evidence.
↑	↑	↑	51F Ozaki	↑	Error correction of the others. Deletion of URLs.
Δ6	2.0	Jun.23, 2020	46F Sugano	1.2.	Deletion of overview.
↑	↑	↑	↑	↑	Addition of position and the figure of the application phase for this document.
↑	↑	↑	↑	1.3.	Correction of Explanations of Acronyms and Terms.
↑	↑	↑	↑	1.4.	Correction of related documents.
↑	↑	↑	↑	2.1.	Addition of the section on conclusion CIAD between Toyota and supplier.
↑	↑	↑	↑	3.	Addition of the chapter on targets and application conditions of this document.
↑	↑	↑	↑	4.2.	Deletion of the description about “Attack port search test” from the evaluation overview of vulnerability countermeasures.
↑	↑	↑	↑	5.1.	Addition of the requirement for evidence creation deadlines.
↑	↑	↑	↑	5.2.1.	Changed the standards that cryptographic algorithms should comply with from CRYPTREC to FIPS, SP800-140C and SP800-140D. Addition of Key length requirements.
↑	↑	↑	↑	5.3.1.	Changed the password length of the countermeasure requirement (PRV-0002) to 128 bits or more.
↑	↑	↑	↑	↑	The Algorithms and random numbers used in C&R authentication for the countermeasure requirement (PRV-0002) are changed to satisfy "ARG-0001, RND-0001, RND-0002".
↑	↑	↑	↑	5.3.3.	Changed the applicable security level of countermeasure requirements (SCD-0001, SCD-0002).

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		4/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

↑	↑	↑	↑	5.3.5.	Deleted the description “Applicable to the session key only” in the countermeasure requirement (CSP-0005).
↑	↑	↑	↑	5.3.6.	Corrected the notation of evaluation requirements (IFD-0001-R, IFD-0004-R) to match other evaluation requirements.
↑	↑	↑	↑	5.4.1.	The algorithm and random numbers used in C&R authentication for the countermeasure requirement (TAC-0001) are changed to satisfy "ARG-0001, RND-0001, RND-0002".
↑	↑	↑	↑	5.4.2.	Corrected the notation of evaluation requirements (ANL-0001-R, ANL-0004-R) to match other evaluation requirements.
↑	↑	↑	↑	5.4.3.	Addition of Glitch attack countermeasure requirements as the countermeasure requirement (TMP-0008).
↑	↑	↑	↑	↑	Addition of the requirement for timing analysis measures as the countermeasure requirement (TMP-0009).
↑	↑	↑	↑	↑	Corrected the notation of evaluation requirements (TMP-0003-R, TMP-0004-R, TMP-0005-R) to match other evaluation requirements.
↑	↑	↑	↑	6.	Addition of security requirements for off-the-shelf products.
↑	↑	↑	↑	All items	Addition of application conditions to countermeasure requirements and evaluation requirements.
↑	↑	↑	↑	↑	Error correction of the others.
↑	↑	↑	↑	Top page	Rename document, Addition of special note.
↑	↑	↑	↑	All items	Replace requirement ID with VULCMN_XXXXX format.
Δ7	2.1	Dec.18, 2020	46F Sugano	5.3.3.	Changed the application conditions of secure coding.
↑	↑	↑	↑	5.3.5.	Addition of PSP protection requirements.
↑	↑	↑	↑	5.3.6.	Deletion of OS/OSS vulnerability search requirements.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		5/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

↑	↑	↑	↑	All items	Changed security level to Target AP.
↑	↑	↑	↑	↑	Error correction of the others, Description improvement (additional supplements, etc.).
Δ8	2.2	Apr.29, 2021	46F Ishikawa	5.4.3.	Clarified the target of tamper resistance requirements as CSP.
↑	↑	↑	↑	1.3.	Addition of Acronyms (PSP).
↑	↑	↑	↑	3.1. 5.2.2.1. 5.3.6.1. 5.3.6.2.	Correction of description from security level to Target AP.
↑	↑	↑	↑	All pages	Changed the description of the header
↑	↑	↑	↑	5.4.3.1.	Addition of examples of countermeasures for glitch attacks and timing analysis.
↑	↑	↑	↑	All items	Error correction of the others.
↑	↑	↑	↑	All pages	Addition of English translation.
Δ9	2.3	Jul.30, 2021	46F Ishikawa	5.4.6.	Addition of the requirement for access right management.
↑	↑	↑	46F Hayakawa	5.3.1 5.4.1	Addition of the requirement for password set by string
↑	↑	↑	↑	5.2.1	Addition of the requirement for use of CSP
↑	↑	↑	↑	5.3.6	Addition of the requirement for login function
↑	↑	↑	46F Kiyokawa	4.1	Clarify the IP services over IP ports that are applicable to privileged functions
↑	↑	↑	↑	5.3.1.1	Clarify the conditions for remaining privileged functions
Δ 10	2.4	Aug.31, 2021	46F Kakiya	5.3.6	Addition of the requirement for password of login function
↑	↑	↑	↑	↑	Addition of the requirement for password of an app.
↑	↑	↑	46F Tamaki	5.3.5.1	Changed the Target AP, Application conditions and Requirements of using security IP requirement
↑	↑	↑	46F Ishikawa Hayakawa	5.2.2	Changed the entropy requirement of random numbers used for C&R authentication
↑	↑	↑	↑	5,3,1	Integrated the penalty requirement (VULCMN_00600) for authentication failure in the

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		6/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

					privileged functions without opening in-vehicle parts into the 5.2.2 random numbers requirement (VULCMN_00200), and deleted this requirement.
↑	↑	↑	46F Ishikawa	5,3,6	Changed the application conditions of access right management requirements (VULCMN_03700)
Δ11	2.5.	Sep.23, 2021	46F Kakiya	1.3	Addition of the definition for Application in explanations of terms
↑	↑	↑	46F Tamaki	3.1	Addition of the reference to the definition of target AP
Δ12	2.6	Oct.19, 2021	46F Yasue	3.3	Added list of requirements
↑	↑	↑	46F Tamaki	4.3.4	Deletion of VULCMN_01500
↑	↑	↑	↑	4.2.2	Addition of the requirement related to SP800-90
↑	↑	↑	46F Hayakawa	1.3 1.4	Change the chapter structure and clarify the content of scope and description of requirements
↑	↑	↑	46F Kakiya	1.5 1.6	Changed the explanations of abbreviations and terms.
↑	↑	Nov. 5, 2021	46F Tamaki	4.3.1.1	Clarify the conditions for remaining privileged functions
↑	↑	↑	↑	1.2	Deletion of Fig. 1-1.
↑	↑	↑	↑	All items	Delete evidence requirements.
↑	↑	↑	↑	4.4.3.1 4.4.3.2	Deletion of VULCMN_03100, VULCMN_52100
↑	↑	Nov. 8, 2021	46F Kakiya	1.6 4.3.1.1	Reflect the content of “Information Security Privilege Function List” in this document and delete the above document from the list of related documents.
↑	↑	↑	46F Tamaki	4.3.6	Deletion of VULCMN_02400, VULCMN_51500,
↑	↑	↑	↑	4.2.2.1	Addition of the class in case of using true random number generator
Δ13	2.7	Mar. 1, 2022	46F Tamaki	4.3.5.1	Integrate session key protection requirement (VULCMN_02000) into CSPs / PSPs storage requirement(VULCMN_01702) and remove session key protection requirement (VULCMN_02000)
↑	↑	Mar. 17, 2022	↑	4.3.5.1 4.4.1.1	Change terms from “security IP” to “HSM”

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		7/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

↑	↑	Spr. 29, 2022	↑	4.3.5.1	Clarify terms for secure memory, general-purpose CPU and general-purpose memory
↑	↑	↑	↑	↑	Improve description of protection requirement for CSPs/PSPs
↑	↑	May. 12, 2022	46F Kakiya	4.2.2.1	Correct editorial errors.
↑	↑	May. 17, 2022	46F Tamaki	4.3.5.1	Clarify the application conditions and the requirements for protection requirement of password (VULCMN_01600)
↑	↑	Jun. 16, 2022	↑	4.2.2.1	Clarify the cryptographic algorithm using with random number generators
↑	↑	Jun. 22, 2022	46F Ishikawa	4.3.3.1	Corresponds to revisions of TSC7030G and TSC7047G (add application of CERT-C and CERT-C++)
↑	↑	Jun. 24, 2022	46F Yasue	4.2.2.1 4.3.1.1 4.3.2.1 4.3.4.1 4.3.6.1 4.4.1.1	Clarify English expression in Supplement, Example and Reasons (VULCMN_00200, VULCMN_00800, VULCMN_01100, VULCMN_01400, VULCMN_02200, VULCMN_02503)
Δ14	2.7	Jun. 30, 2022	46F Tamaki	4.2.2.1	Deletion of the requirement about Prediction Resistance of SP800-90A
↑	↑	Aug. 11, 2022	↑	↑	Correction of the requirement for 128bit random number strings collision
↑	↑	Oct. 25, 2022	↑	4.3.6.1	Clarify the requirement for TCP/UDP ports (VULCMN_02100)
↑	↑	↑	↑	4.3.2.1	Clarify the requirement for specifications not specified by Toyota Motor Corporation (VULCMN_01000)
↑	↑	↑	↑	Cover page	Change format
↑	↑	↑	46F Kiyokawa	4.3.5.1	Clarify the requirement for the protection of PSPs. (VULCMN_01701, VULCMN_01702)
Δ15	a01-08-a	Nov. 10, 2022	46F Tamaki	5.1	Deletion of the requirement “Unit test for off-the-shelf products(VULCMN_52300)”
↑	↑	↑	↑	2.1	Change terms from CIAD to CIA
↑	↑	Nov. 17, 2022	46F Yasue	4.3.1.1	Add the privileged functions permitted by the department responsible for

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		8/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

					security(VULCMN_00400)
Δ16	a01-09-a	Jan. 13, 2023	46F Tamaki	4.3.2.2	Clarify the evaluation requirement for specifications not specified by Toyota Motor Corporation (VULCMN_50600)
↑	↑	Jan. 25, 2023	↑	1.6	Deletion of the Deleted Document
↑	↑	↑	↑	3.3	Correct errors in Table 3-5
↑	↑	↑	↑	3.1	Addition of the description of the IP services
↑	↑	Feb. 14, 2023	46F Kiyokawa	4.4.3	Clarify the applicable target.
↑	↑	Mar. 27, 2023	46F Yasue	4.3.3	Clarify the secure cording requirement (VULCMN_01200, VULCMN_50800, deleted VULCMN_50900)

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		9/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

Table of Contents

1. INTRODUCTION	11
1.1. PURPOSE OF THIS DOCUMENT	11
1.2. POSITION OF THIS DOCUMENT ^{Δ6Δ12}	11
1.3. SCOPE ^{Δ12}	11
1.4. DESCRIPTION OF REQUIREMENTS ^{Δ12}	11
1.5. EXPLANATIONS OF ABBREVIATIONS AND TERMS ^{Δ12}	12
1.6. RELATED DOCUMENTS	13
2. PRECONDITIONS FOR THIS DOCUMENT^{Δ6}	16
2.1. CONCLUSION CIA BETWEEN TOYOTA AND SUPPLIERS ^{Δ6Δ14}	16
3. OVERVIEW OF VULNERABILITY COUNTERMEASURES	17
3.1. OVERVIEW OF VULNERABILITY COUNTERMEASURES	17
3.2. EVALUATION OVERVIEW OF VULNERABILITY COUNTERMEASURES ^{Δ6}	25
3.3. LIST OF REQUIREMENTS ^{Δ12}	26
3.4. CORRESPONDENCE BETWEEN COUNTERMEASURE REQUIREMENTS AND EVALUATION REQUIREMENTS	29
4. REQUIREMENTS FOR VULNERABILITY COUNTERMEASURES AND EVALUATION OF VULNERABILITY COUNTERMEASURES^{Δ1Δ6Δ7}	31
4.1. COMMON REQUIREMENTS ^{Δ6}	31
4.2. COUNTERMEASURES FOR ENCRYPTION ALGORITHMS AND RANDOM NUMBERS	32
4.2.1. Encryption Algorithms	32
4.2.2. Random Numbers	34
4.3. RESISTANCE TO CLOSED ATTACKS ON IN-VEHICLE PARTS	39
4.3.1. Countermeasures for Privileged Functions of In-vehicle Parts without Opening (Debug, Maintenance)	39
4.3.2. Countermeasures in Specifications	46
4.3.3. Secure Coding	49
4.3.4. Protection Measures for Programs/Data (Protection of Programs)	52
4.3.5. Protection Measures for Programs/Data (Protection of CSPs • PSPs)	53
4.3.6. Protection Measures for Programs and Data (Protection of Data for Information-related In-vehicle Parts)	57
4.4. RESISTANCE TO OPEN ATTACKS ON IN-VEHICLE PARTS	62
4.4.1. Countermeasures for Privileged Functions of In-vehicle Parts by Opening (Test Access Port)	62

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		10/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

4.4.2.	Countermeasures against PCB Analysis.....	65
4.4.3.	Tamper Resistance.....	67
5.	DELETED ^{Δ6 Δ14}	70
5.1.	DELETED ^{Δ6 Δ14}	70

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		11/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

1. Introduction

1.1. Purpose of This Document

The purpose of this document is to provide the minimum vulnerability countermeasure requirements to mitigate the vulnerabilities common among in-vehicle parts.

1.2. Position of This Document ^{Δ6Δ12}

Similar to this document, Table 1-1 List of requirements for reducing vulnerabilities^{Δ6} shows a list of countermeasure requirements / evaluation requirements and the position of each document in order to build an ECU without vulnerabilities^{Δ6}.

Table 1-1 List of requirements for reducing vulnerabilities^{Δ6}

The name of the document	Position
Requirements specification of vulnerability countermeasure for ECU	In each architecture design process in ECU development, Define requirements for vulnerability analysis and vulnerability countermeasures.
Test specification of vulnerability countermeasure for ECU	In each test process in ECU development, Define requirements for evaluating security-related features (including vulnerability assessments).
Requirements Specification of Common Vulnerability Countermeasure (This document)	To make it difficult for an attacker to find a vulnerability, Define vulnerability countermeasures that each ECU should take in common during the design/evaluation and implementation process.

1.3. Scope^{Δ12}

To prevent vehicle hacking, Toyota instructs the ECU located on the attack path to assign the security specifications. The scope of this document is an ECU that is instructed to develop one of the security functions. ^{Δ6}

1.4. Description of Requirements^{Δ12}

In order to reduce security risks to acceptable levels by vulnerability countermeasures, it is necessary to apply vulnerability countermeasures according to the Target Attack Potential (subsequently described as "Target AP")^{Δ7}. The following two items are defined as the application conditions for each requirement of this document. The ECU designer shall check each requirement and implement the requirements that apply to own condition. ^{Δ6}

- ① Functions/Parts : Whether to use specific functions(wireless communication function, etc.)/specific parts(off-the-shelf products, etc.)

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		12/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

- ② Target AP : The value given to the cybersecurity requirement that is assigned to each ECU (※) ^{Δ11}

※ The definition of target AP is described in “Requirements specification of vulnerability countermeasure for ECU” ^{Δ11}.

1.5. Explanations of Abbreviations and Terms ^{Δ12}

The Abbreviations to be used in this document are defined as follows.

Table 1.2 List of Abbreviations ^{Δ12}

AcronymAbbreviation	Explanation
CAVP	Cryptographic Algorithm Validation Program http://csrc.nist.gov/groups/STM/cavp/

The explanations of the terms and the defined terms used in this document are given below.

Table 1.3 List of Terms and Defined Terms ^{Δ12}

Term	Explanation
Compromise	A circumstance in which the safety level of security is adversely affected by some sort of action or change of the condition. E.g. Leakage of encryption keys, deterioration of safety of encryption algorithms due to improved computer processing capabilities
Privilege mode	The mode which permits unlimited CPU processing. This mode is capable of running any command, starting any input/output operations, and accessing any memory location. This mode is also known as “kernel mode” and “supervisor mode”.
User mode	Non-privilege mode whose capabilities to run commands and access to memory locations are limited and input/output operations are disabled.
Specifications specified by Toyota Motor Corporation ^{Δ2}	The one which is specified with the requirements specification described on “REQUEST FOR DESIGN & DEVELOPMENT OF PARTS (RDDP)” for the In-vehicle parts issued by Toyota Motor Corporation. ^{Δ2}
Authentication data ^{Δ4}	The data which is treated by an entity to require authentication and an entity to be required for authentication in the process (Authentication) of establishing confidence in the identity of users or information systems. It includes ID, Password and Certificate. ^{Δ4}
Random number seed ^{Δ4}	The input to a pseudorandom number generator. Different seeds generate different pseudorandom sequences. ^{Δ4}

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		13/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

Application	A software which is performed on OS is complied with POSIX OS or AGL and provides services, a payment service or entertainment function etc., for customers.
-------------	--

1.6. Related Documents

The documents related to this document are as follows.

Table 1.4 List of Related Documents^{Δ1Δ5Δ6}

Specification Number	Title
(Delete) ^{Δ16}	
SEC-ePF-VUL-ECU-REQ-SPEC ^{Δ6}	Requirements specification of vulnerability countermeasure for ECU ^{Δ6}
SEC-ePF-VUL-ECU-TST-SPEC ^{Δ6}	Test specification of vulnerability countermeasure for ECU ^{Δ6}
wguide ^{Δ5}	Constitution of Diagnostics ^{Δ2}
SEC-ePF-RPR-REQ-SPEC ^{Δ6}	Requirements Specification of Standard Reprogramming Security
SEC-ePF-PPI-REQ-SPEC ^{Δ6}	Requirements of Personal and Privacy Information for Post19PF ^{Δ5Δ6}
SEC-ePF-TRM-GUD-PROC Δ12	Terms and Definitions related to Vehicle Cybersecurity and Privacy

*) Table 1.4 List of related documents will be updated in the future^{Δ6}

Table 1.5 List of Public Related Documents^{Δ1Δ5}

Abbreviation in this document ^{Δ5}	Title and External link
CAVP ^{Δ5}	Cryptographic Algorithm Validation Program http://csrc.nist.gov/groups/STM/cavp/
AIS20 ^{Δ5}	Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_Functionality_Classes_Evaluation_Methodology_DRNG_e.pdf?__blob=publicationFile&v=1
KS2011 ^{Δ5}	A proposal for: Functionality classes for random number generators https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile&v=1 ^{Δ4} * This document is with AIS20 and AIS31 integrated ^{Δ5} .
AIS31 ^{Δ5}	A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_evaluation_methodology_for_true_RNG_e.pdf?__blob=publicationFile&v=1

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		14/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

ISO/IEC TR 24772 ^{Δ5}	Information technology -- Programming languages -- Guidance to avoiding vulnerabilities in programming languages through language selection and use http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61457
CERT-C ^{Δ5}	SEI CERT C Coding Standard https://www.securecoding.cert.org/confluence/display/c/SEI+CERT+C+Coding+Standard
CERT-C++ ^{Δ5}	SEI CERT C++ Coding Standard https://www.securecoding.cert.org/confluence/pages/viewpage.action?pageId=637
CERT-JAVA ^{Δ5}	SEI CERT Oracle Coding Standard for Java https://www.securecoding.cert.org/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java
CERT-Perl ^{Δ5}	SEI CERT Perl Coding Standard https://www.securecoding.cert.org/confluence/display/perl/SEI+CERT+Perl+Coding+Standard
ISO/SAE 21434 ^{Δ6}	ISO/SAE DIS 21434 Road vehicles — Cybersecurity engineering https://www.iso.org/standard/70918.html
ISO/IEC 19790 ^{Δ6}	Information technology – Security techniques – Security Requirements for Cryptographic Modules http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52906
SP800-57 ^{Δ6}	Recommendation for Key Management: Part1 General https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
SP800-140C ^{Δ6}	CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140C.pdf
SP800-140D ^{Δ6}	CMVP Approved Sensitive Security Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140D.pdf
FIPS	Federal Information Processing Standards https://csrc.nist.gov/publications/fips
WP29 ^{Δ6}	A new UN Regulation on Cyber security https://www.unece.org/trans/main/wp29/meeting_docs_grva.html

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		15/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

(Note 1)

Follow the contents of the latest specifications.

(Note 2)

If there is a discrepancy between the present specifications/related specifications and the specifications issued by Toyota design department, the contents of those documents shall be confirmed. Therefore, contact the department responsible for security (the department that issued the present specifications) and Toyota design department that issued the specifications to be confirmed.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		16/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

2. Preconditions for this document^{Δ6}

This document defines the requirements for creating an ECU without vulnerability.

2.1. Conclusion CIA between Toyota and suppliers^{Δ6Δ15}

When starting the development of the ECU, Toyota issues the REQUEST FOR DESIGN & DEVELOPMENT OF PARTS (subsequently described as “RDDP”) to the supplier, it directs the specifications (including security-related specifications) to be assigned to the ECU. ^{Δ6}

In order to comply with ISO/SAE 21434, By the date the RDDP is issued, the division of roles / responsibilities between Toyota and the supplier will be clarified and a CIA (Cybersecurity Interface Agreement)^{Δ15} will be concluded. The CIA^{Δ15} concluded is attached to the RDDP in addition to the security-related specifications. ^{Δ6}

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		17/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

3. Overview of Vulnerability Countermeasures

3.1. Overview of Vulnerability Countermeasures

Devices that require security functions are susceptible to analyses and attacks. In general, when attacking a security system, attackers analyze the device and attempt to find vulnerabilities. Then those vulnerabilities are exploited and attacked.

To mitigate the analysis and attack-related risks, it is important to design and implement security functions to minimize vulnerabilities that are likely to be exploited by attackers and design and implement the security functions whose vulnerabilities are difficult to find. In other words, design and implementation of security functions that are difficult to analyze is important.

This document aims to reduce vulnerabilities and prevent analyses.

The figure below (Fig. 3-1 Analysis and Attack Ports of In-vehicle Part (ECU)) visualizes analysis and attack ports of an in-vehicle part (ECU). On the assumption that the programs and the data stored in the in-vehicle part are the assets to protect, the figure shows the types of analyses and attacks.

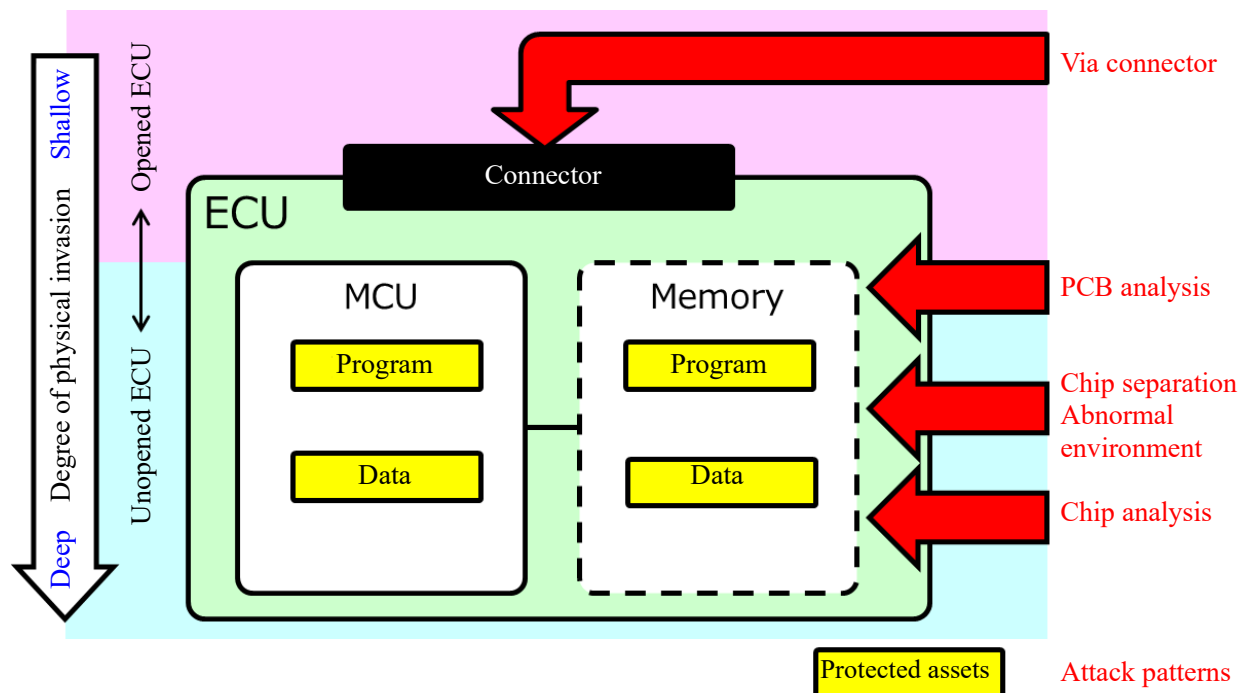


Fig. 3-1 Analysis and Attack Ports of In-vehicle Part (ECU)

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		18/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

The ports, overviews, and explanations of the analyses and attacks are given in Table 3-1 Ports, Overviews, and Explanations of Analyses and Attacks.

Table 3-1 Ports, Overviews, and Explanations of Analyses and Attacks

Port		Overview	Explanation
In-vehicle parts without opening (analyses and attacks)	Via connector	Exploitation of flaws in encryption algorithms and random numbers	- Analysis/attack exploiting flaws in encryption algorithm specifications and random number specifications and inadequate operations of such specifications
		Exploitation of privileged functions	The following analysis/attack from privileged function connected to connector and wireless of in-vehicle parts interface or privileged functions connected via global bus ^{Δ4} - Access to the data using the diagnostics function (read and rewrite) - Access to the data using the calibration function of CAN, etc. (read and rewrite) - Reprogramming using the reprogramming function - Access to information assets using the function for inspection of supplier's product - IP services that allows to execute commands from the outside ^{Δ9}
		Software analysis	- Process hijacking, malware injection, internal information analysis, etc. exploiting vulnerabilities of the implemented software
In-vehicle parts by opening (analyses)	PCB analysis	Exploitation of privileged functions	- Exploitation of test access ports (JTAG, etc.), analysis, reprogramming - Exploitation of microcontroller test mode, analysis, reprogramming
		PCB surface probing	- Probing of wires: Wiretapping and analysis of chip-to-chip communication - Hacking through terminals, data reading and rewriting
	Chip separation	Chip replacement	- Reprogramming by replacing chips - Chip is removed from the PCB and is analyzed.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		19/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

	Abnormal environment	Noise injection (fault attack)	- Malfunction is caused by irradiating a laser or injecting noise and analysis is performed.
	Chip analysis	Side-channel attack	- Guessing of the encryption key by measuring the electromagnetic wave and current from outside the chip, etc.
		Destructive analysis (invasive attack)	- Destructive analysis and analysis using an electron microscope of chips, probing of silicon dies

The correspondence between the analysis/attack overviews and the countermeasure overviews is given in Table 3-2.

Table 3-2 Correspondence between Analysis/Attack Overviews and Countermeasure Overviews

Countermeasure overview Analysis/attack overview		Countermeasures for encryption algorithms and random numbers	Countermeasures for privileged functions in in-vehicle parts without opening (debug and maintenance)	Countermeasures in specifications	Secure coding	Protection measures for programs and data	Countermeasures for privileged functions in in-vehicle parts by opening (test access port)	Countermeasures against PCB analysis	Tamper resistance
In-vehicle parts without opening (analysis/attack)	Exploitation of flaws in encryption algorithms and random numbers	○							
	Exploitation of privileged functions		○			○			
	Software analysis			○	○	○			
In-vehicle parts by opening (analysis)	Exploitation of privileged functions					○	○		
	PCB surface probing					○		○	
	Chip replacement					○			
	Noise injection								○
	Side-channel attack								○
	Destructive analysis of chip								○

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		20/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

Analyses and attacks, parts of those analyses and attacks, and countermeasures for those analyses and attacks will be explained in this section. (In the following sections analyses and attacks will be correctively referred to as “attacks”.) In-vehicle parts shall incorporate appropriate measures for their Target AP^{Δ7}.

Via connector

■ Attack: Exploitation of flaws in encryption algorithms and random numbers

Flaws in encryption algorithm specifications and insufficient consideration when selecting random number specifications and inadequate operations of such specifications can be potentially exploited. Therefore, measures against such attacks shall be taken.

◇ Countermeasure: Countermeasures for encryption algorithms and random numbers

Select encryption algorithms and random numbers that are specified by Toyota Motor Corporation that they have been verified to be free of vulnerabilities and confirm that they operate adequately with the in-vehicle parts.

■ Attack: Exploitation of privileged functions in in-vehicle parts without opening (debug and maintenance)

Privileged functions are the debug and maintenance functions that give the user access^{Δ4} to the programs and data stored in the in-vehicle part.

Case to connect privileged functions to connector of in-vehicle parts interface, case to connect privileged functions via global bus, or case to connect privileged functions via wireless communication are applicable to privileged functions without opening. ^{Δ4Δ9}

As privileged functions without opening, in the above case, ^{Δ4} read and write of memories using the diagnostics^{Δ4}, read and write of data using the CCP/XCP^{Δ7}, reprogramming using the reprogramming function, access to information assets using the product inspection function by the supplier, and operate from the outside using^{Δ16} IP services that allows to execute commands from the outside (telnet, ssh, dbus, Android Debug Bridge, etc) ^{Δ9} are the examples.

While these functions are crucial functions throughout the life cycle of products including the development phase, the production phase, the maintenance phase, the fault analysis phase, and the disposal phase, it is a very convenient backdoor from the standpoint of attackers and because it can be potentially used as a means for attacks including disabling security functions through reading programs and data, reading and rewriting of encryption keys, and reprogramming, countermeasures against such attacks shall be taken.

◇ Countermeasure: Countermeasures for privileged functions of In-vehicle parts without opening (debug, maintenance)

Disable the privileged function or control the access rights with use of an authentication means.

Note that when an encryption key is shared by more than one in-vehicle part, leakage of the encryption key of one in-vehicle part affects other parts. Give consideration to prevent effects on other vehicles by using different encryption keys for different vehicles according to the Target AP^{Δ7}, using unique encryption keys for each of all

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		21/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

the in-vehicle parts in the vehicle, and the like.

◇ Countermeasure: Protection measures for programs and data^{Δ12}

It is feasible to detect tampering of programs or data by checking the integrity of the data prior to running the program or using the data. Ensure to incorporate this measure in in-vehicle parts with the reprogramming function.

In addition, to prevent the privileged functions from being exploited by attackers, programs and data (specifically CSP・PSP^{Δ7} such as encryption keys, etc.) can be protected with use of a secure microcontroller, etc. Take measures appropriate for the Target AP^{Δ7}.

The countermeasure explanations are added to the section explaining program/data protection against attacks of in-vehicle parts without opening after Chapter 5.

■ Attack: Software analysis

When implementation of software or settings of OS and hardware have flaws, they potentially leave room for attacks such as hijacking of processes, injection of malware, and elevation of rights. Therefore, measures against such attacks shall be taken.

◇ Countermeasure: Countermeasures in specifications

Prevent inclusion of functions that potentially have vulnerabilities through clarifying software functions and excluding unnecessary functions.

◇ Countermeasure: Secure coding

To prevent inclusion of vulnerabilities at the time of software implementation, implement software in compliance with the secure coding rules. Take measures appropriate for the Target AP.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		22/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

◇ Countermeasure: Protection measures for programs and data

See the section explaining the “Protection measures for programs and data” via connectors for details of the countermeasure.

PCB analysis

■ Attack: Exploitation of privileged functions of in-vehicle parts by opening (test access port)

Microcontrollers have test access ports including JTAG port for debug, maintenance, manufacturing, and other purposes. Because this function is standardized by the IEEE and provides direct access to the resources inside the microcontroller, it is a good backdoor for attackers and can be potentially used for attacks including reading of programs and data, reading/writing of encryption keys, and disabling security functions by tampering of the program. Therefore, measures against such attacks shall be taken.

◇ Countermeasure: Protection measures for programs and data

See the section explaining the “Protection measures for programs and data” via connectors for details of the countermeasure.

◇ Countermeasure: Countermeasures for privileged functions of In-vehicle parts by opening (test access port)

Disable the privileged functions or implement access control by authentication. Generally speaking, test access ports of microcontrollers have an authentication function using passwords in many cases. If a password is shared by all in-vehicle parts, leakage of the password affects all other in-vehicle parts. Establish a password difficult to guess for each in-vehicle part. Take measures appropriate for the Target AP^{Δ7}.

■ Attack: PCB surface probing

Attacks such as wiretapping by probing wires from the surface layer of the PCB, and analysis and reading/rewriting of behaviors by accessing chips from chip terminals or points connected to terminals are conceivable. Specifically when storing the program on an external memory (flash memory, etc.), reading and rewriting via terminals can be performed easily. Therefore, measures against such attacks shall be taken.

◇ Countermeasure: Protection measures for programs and data

See the section explaining the “Protection measures for programs and data” via connectors for details of the countermeasure.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		23/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

◇ Countermeasure: Countermeasures against PCB analyses

Encrypt contents of chip-to-chip communication to prevent analysis of confidential information. When storing CSPs^{Δ4} in an external memory due to some restrictions, encrypt them in the microcontroller prior to storing. It is not necessary to handle all information communicated as confidential information, and implement this countermeasure only to prevent leakage of confidential information (CSPs^{Δ4} in this context) and analysis of the security functions. Take measures appropriate for the Target AP^{Δ7}.

Chip separation

■ Attack: Chip replacement

When the program is stored on an external memory, the program can be potentially tampered by replacing the external memory chip. Therefore, measures against such attack shall be taken.

◇ Countermeasure: Protection measures for programs and data

See the section explaining the “Protection measures for programs and data” via connectors for details of the countermeasure.

Abnormal environment

■ Attack: Noise injection

There are attacks involving malfunction of chips by irradiating a laser, causing clock glitch, voltage drop, or the like, and messing up IF statement branches of programs to achieve successful authentication using any random number. Therefore, measures against such attacks shall be taken.

◇ Countermeasure: Tamper resistance

Resistance against physical analyses using noise detection and layout and resistance against side-channel attacks are effective. Take measures appropriate for the Target AP^{Δ7}.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		24/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

Chip analysis

■ Attack: Side-channel attack

There is a potential attack of guessing the encryption key by measuring the electromagnetic wave and consumption current during encryption operation and running statistical processing. Therefore, measures against such attack shall be taken.

◇ Countermeasure: Tamper resistance^{Δ1}

See the countermeasure for abnormal environment for the explanation. ^{Δ1}

■ Attack: Destruction analysis of chips

There are potential attacks of destructing a chip and analyzing the contents of the processing by analyzing the layout and wiring information with use of an electron microscope, etc., reading confidential information by reading the ROM and directly probing the wiring of silicon dies, and modifying circuits by FIB. Therefore, measures against such attacks shall be taken.

◇ Countermeasure: Tamper resistance

See the countermeasure for abnormal environment for the explanation.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		25/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

3.2. Evaluation Overview of Vulnerability Countermeasures^{Δ6}

The product with vulnerability countermeasure should be evaluated that the countermeasure is implemented appropriately and does not contain unacceptable vulnerabilities. The evaluation of vulnerability countermeasures is to conduct design verification, source code review, etc. for each vulnerability countermeasure, and to check whether the measures are accurately reflected in the design and implementation. Table 3-3 Evaluation Overview of Vulnerability Countermeasures^{Δ1} provides an evaluation overview of vulnerability countermeasures that addresses the vulnerability countermeasure overview.^{Δ6}

Table 3-3 Evaluation Overview of Vulnerability Countermeasures^{Δ1Δ6}

Overview of Vulnerability Countermeasures	Evaluation Overview of Vulnerability Countermeasures ^{Δ1Δ6}
Countermeasures for encryption algorithms and random numbers	Encryption algorithms and random numbers standard check
Countermeasures for privileged functions of in-vehicle parts without opening (debug, maintenance)	Countermeasures for privileged functions in in-vehicle parts without opening (debug and maintenance) check
Countermeasures in specifications	Countermeasures in specifications check
Secure coding	Secure coding check
Protection measures for programs and data	Protection measures for programs and data check
Countermeasures for privileged functions of in-vehicle parts by opening (test access port)	Countermeasures for privileged functions in in-vehicle parts by opening (test access port) check
Countermeasures against PCB analysis	Countermeasures against PCB analysis check
Temper resistance	Tamper resistance check

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		26/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

3.3. List of Requirements^{Δ12}

The requirement items defined in this document are shown in Table 3-4. For detail of each Requirements, refer to chapter 4 and later.

The requirements to which ECU designer should refer in selecting hardware are marked with "○" in the "Hardware-related requirements" column.

Table 3-4 List of Requirements

Classification	Requirement	Hardware-Related Requirements
Common Requirements	VULCMN_52400(Deleted)	-
Countermeasures for Encryption Algorithms and Random Numbers	VULCMN_00100	-
	VULCMN_03600	-
	VULCMN_50100	-
	VULCMN_52500	-
	VULCMN_00200	○
	VULCMN_00300	-
	VULCMN_50200	-
	VULCMN_50300	-
Resistance to Closed Attacks on In-vehicle Parts	VULCMN_00400	-
	VULCMN_00500	-
	VULCMN_00501	-
	VULCMN_00502	-
	VULCMN_00503	-
	VULCMN_00600(Deleted)	-
	VULCMN_00700	-
	VULCMN_00800	-
	VULCMN_00900	-
	VULCMN_50400	-
	VULCMN_50500	-
	VULCMN_01000	-
	VULCMN_01100	-
	VULCMN_50600	-
	VULCMN_50700	-
	VULCMN_01200	-
	VULCMN_01300	-

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		27/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

	VULCMN_50800	-
	VULCMN_50900(Deleted)	-
	VULCMN_51000	-
	VULCMN_01400	-
	VULCMN_01500(Deleted)	-
	VULCMN_51100	-
	VULCMN_01600	-
	VULCMN_01700	○
	VULCMN_01701	-
	VULCMN_01702	○
	VULCMN_01800	-
	VULCMN_01900	-
	VULCMN_02000(Deleted) ^{Δ13}	-
	VULCMN_51200	-
	VULCMN_02100	-
	VULCMN_02200	-
	VULCMN_02300	-
	VULCMN_02400(Deleted)	-
	VULCMN_03700	-
	VULCMN_03800	-
	VULCMN_03900	-
	VULCMN_04000	-
	VULCMN_51300	-
	VULCMN_51400	-
	VULCMN_51500(Deleted)	-
	VULCMN_52600	-
	VULCMN_52700	-
	VULCMN_52800	-
	VULCMN_52900	-
Resistance to Open Attacks on In-vehicle Parts	VULCMN_02500	-
	VULCMN_02501	-
	VULCMN_02502	-
	VULCMN_02503	-
	VULCMN_02600	-
	VULCMN_02601	-

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		28/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

	VULCMN_02602	○
	VULCMN_51600	-
	VULCMN_51700	-
	VULCMN_02700	○
	VULCMN_02800	-
	VULCMN_51800	-
	VULCMN_51900	-
	VULCMN_02900	○
	VULCMN_03000	○
	VULCMN_03100(Deleted)	○
	VULCMN_03200	○
	VULCMN_03300	○
	VULCMN_03400	○
	VULCMN_03500	○
	VULCMN_52000	-
	VULCMN_52100(Deleted)	-
	VULCMN_52200	-
Security evaluation for off-the-shelf products	VULCMN_52300(Deleted)	-

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		29/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

3.4. Correspondence between Countermeasure Requirements and Evaluation Requirements

The evaluation requirements are given in Chapter 5 along with the countermeasure requirements. IDs are assigned to those items and they help associate the countermeasure requirements with the evaluation requirements. Make sure to carry out an evaluation for all countermeasure requirements.

The correspondence between the countermeasure requirements and the evaluation requirements is shown in Table 3-5 Countermeasure Requirement-Evaluation Requirement Correspondence.

Table 3-5 Countermeasure Requirement-Evaluation Requirement Correspondence^{A6}

Overview of Vulnerability Countermeasures	Countermeasure requirement (ID)	Evaluation requirement (ID)
Countermeasures for encryption algorithms and random numbers	VULCMN_00100, VULCMN_00200, VULCMN_00300, VULCMN_03600 ^{A16}	VULCMN_50100 ^{A4} , VULCMN_50200 ^{A4} , VULCMN_50300 ^{A4} , VULCMN_52500 ^{A16}
Countermeasures for privileged functions of In-vehicle parts without opening (debug, maintenance)	VULCMN_00400, VULCMN_00500, VULCMN_00501, VULCMN_00502, VULCMN_00503, VULCMN_00700, VULCMN_00800, VULCMN_00900	VULCMN_50400 ^{A4} , VULCMN_50500
Countermeasures in specifications	VULCMN_01000, VULCMN_01100	VULCMN_50600 ^{A4} , VULCMN_50700 ^{A4}
Secure coding	VULCMN_01200, VULCMN_01300	VULCMN_50800, VULCMN_51000 ^{A4}
Protection measures for programs and data	VULCMN_01400, VULCMN_01600, VULCMN_01700, VULCMN_01701, VULCMN_01702, VULCMN_01800, VULCMN_01900, VULCMN_02100, VULCMN_02200, VULCMN_02300, VULCMN_03700 ^{A9} , VULCMN_03800 ^{A9} , VULCMN_03900 ^{A10} , VULCMN_04000 ^{A10}	VULCMN_51100 ^{A4} , VULCMN_51200 ^{A4} , VULCMN_51300 ^{A4} , VULCMN_51400 ^{A4} , VULCMN_52600 ^{A9} , VULCMN_52700 ^{A9} , VULCMN_52800 ^{A10} , VULCMN_52900 ^{A10}
Countermeasures for privileged functions of In-vehicle parts by opening (test access port)	VULCMN_02500, VULCMN_02501, VULCMN_02502, VULCMN_02503, VULCMN_02600	VULCMN_51600, VULCMN_51700
Countermeasures against PCB analysis	VULCMN_02700, VULCMN_02800	VULCMN_51800 ^{A4} ,

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		30/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

		VULCMN_51900 ^{Δ4}
Tamper resistance	^{Δ5} VULCMN_02900, VULCMN_03000, VULCMN_03200, VULCMN_03300, VULCMN_03400, ^{Δ6} VULCMN_03500 ^{Δ6}	^{Δ5} VULCMN_52000 ^{Δ4} , VULCMN_52200 ^{Δ6}

Note: For details, please check each requirement item after Chapter 5.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		31/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

4. Requirements for vulnerability countermeasures and evaluation of vulnerability countermeasures^{Δ1Δ6Δ7}

This chapter describes the requirements for vulnerability countermeasures and evaluation of vulnerability countermeasures.

Regarding the application of each requirement, first, check the Application conditions for each requirement. If the ECU meets the Application conditions, check the Target AP of the requirement. If the Target AP of the security function installed in the ECU fits the Target AP of the requirement, apply the requirement to the ECU.

(The requirements applied to the ECU are described as “Application requirements”).^{Δ7}

4.1. Common Requirements^{Δ6}

This section provides common requirements for each requirements set out in this chapter.

Requirements for evidence creation deadlines^{Δ6}

ID		VULCMN_52400
Application conditions ^{Δ12}	Functions/Parts	-
	Target AP ^{Δ7}	-
Requirements		Deleted.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		32/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

4.2. Countermeasures for Encryption Algorithms and Random Numbers

The countermeasure requirements and evaluation requirements for the implementation of cryptographic algorithms and random numbers, which are the major premise of security, are shown.

4.2.1. Encryption Algorithms

4.2.1.1. Countermeasure Requirements

Attacks exploiting vulnerabilities of cryptographic algorithms shall be prevented.

ID		VULCMN_00100 ^{Δ6}
Application	Functions/Parts	ECUs using encryption algorithms
conditions ^{Δ6Δ12}	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements ^{Δ6}		<p>The ECU shall use the cryptographic algorithm listed in "FIPS", "SP800-140C", or "SP800-140D", and whose Status is Final.(*1)</p> <p>*1)Status is “Withdrawn”, “Draft” should not be selected.^{Δ7}</p> <p>In addition, based on "SP800-57", the cryptographic algorithm to be used and the key length should decide that the security strength satisfies 128 bits or more.</p> <p>(Supplement) Below, the key length that is 128 bit security strength for typical common key cryptography, public key cryptography, and MAC is shown.</p> <ul style="list-style-type: none"> ▪ Common key cryptography : AES/128bit ▪ Public key cryptography : RSA/3072bit, ECDSA/256bit, ECDH/256bit ▪ MAC : AES-CMAC/128bit <p>In addition, a typical hash function 128bit security strength is shown below.</p> <ul style="list-style-type: none"> ▪ Hash function : SHA256
Reasons		<p>When using an original algorithm, although it has the same key length having the substantially same encryption strength, it can be potentially inferior to others. The use of widely accepted standards is also required for "WP29", it is necessary to use encryption algorithms that have been under scrutiny of security specialists. ^{Δ6}</p> <p>The encryption algorithm being free of vulnerabilities is the prerequisite of security functions.</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		33/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

ID		VULCMN_03600 ^{Δ9}
Application conditions ^{Δ12}	Functions/Parts	ECUs that use cryptographic keys that require confidentiality(common key, private key) for cryptographic operations related to the cyber security requirements.
	Target AP	All
Requirements		The same cryptographic key shall not be used for multiple purposes in cryptographic processes.
Reasons		Uses of the same cryptographic key for multiple purposes raise concerns about the possibility of the leakage of cryptographic key and the spread of effects when it is leaked.

4.2.1.2. Evaluation Requirements

ID		VULCMN_50100 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs using encryption algorithms
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ6Δ7}
Requirements		<p>This requirement should be implemented when applying VULCMN_00100.</p> <p>The ECU designer shall perform a test (*) equivalent to the known answer test (AESAVS if the encryption algorithm is AES) described in the test vector published by CAVP^{Δ12}, to demonstrate that the encryption algorithm is implemented correctly.^{Δ4}</p> <p>*) When cryptographic module supplied from the vendor is used, either of the followings shall be carried out.^{Δ4}</p> <ul style="list-style-type: none"> - Receive the result of a CAVP-equivalent test performed from the vendor.^{Δ4} - Perform a CAVP-equivalent test for the cryptographic module.^{Δ4}
Items to be checked		Validity of the algorithms

ID		VULCMN_52500 ^{Δ9}
Application conditions ^{Δ12}	Functions/Parts	When VULCMN_03600 is applied.
	Target AP	All
Requirements		The countermeasure requirements shall be satisfied through design verification.
Items to be checked		<p>List of cryptographic keys to be verified</p> <p>Confirm that all cryptographic keys in the above list satisfy the countermeasure requirement</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		34/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.2.2. Random Numbers

4.2.2.1. Countermeasure Requirements

Attacks exploiting vulnerabilities of random numbers shall be prevented.

ID		VULCMN_00200 ^{Δ6}																												
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs with random number generators ^{Δ7}																												
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}																												
Requirements		<p>The random number generator shall be satisfied the requirement of the followings (1) or (2).^{Δ13}</p> <p>(1):^{Δ12Δ13}</p> <ul style="list-style-type: none"> - If the product is equipped with a hardware true random number generator, this generator shall be used (*1). Note that the true random number generator shall comply with AIS31(PTG.2 or PTG.3)^{Δ12}. <p>*1) If the output of the hardware true random number generator can not be directly used, the pseudo random number generator may be used with its output as a random number seed.^{Δ5}</p> <ul style="list-style-type: none"> - When using a pseudo random number generator, the requirement values shall be satisfied according to the Target AP shown below in reference to AIS20. <table> <tr> <th rowspan="2"></th><th rowspan="2">Random Number use case^{Δ3Δ5}</th><th colspan="3">Target AP^{Δ8}</th></tr> <tr> <th>10~13^{Δ8}</th><th>14~19^{Δ8}</th><th>20^{Δ8}</th></tr> <tr> <td rowspan="2">Entropy requirement value (bit)^{Δ4}</td><td>Key generation^{Δ3}</td><td>_^{Δ3}</td><td>80^{Δ3}</td><td>80^{Δ3}</td></tr> <tr> <td>C&R authentication^{Δ3}</td><td>The value shall be determined according to(*2)^{Δ3Δ10}</td><td>The value shall be determined according to (*2)^{Δ3Δ10}</td><td>The value shall be determined according to (*2)^{Δ3Δ10}</td></tr> <tr> <td rowspan="2">Algorithm unpredictability requirement value</td><td>Key generation^{Δ5}</td><td colspan="3">Backward secrecy&Forward secrecy^{Δ5}</td></tr> <tr> <td>C&R authentication^{Δ5}</td><td colspan="3">Forward secrecy(*4)^{Δ5Δ13}</td></tr> </table> <p>(This requirement shall be met in the design in the development phase.)^{Δ6}</p> <p>*2) The designer chooses whether a penalty for authentication failure is necessary and sets the entropy and penalty that satisfy the following formula.</p> <p>If a penalty is not necessary</p> <p>H: Entropy [bit]</p> <p>T: Processing time from C&R authentication challenge request to challenge response (average processing time at one time) [ms]</p> <p>c: Unit conversion coefficient (1000×60×60×24×365)</p>				Random Number use case ^{Δ3Δ5}	Target AP ^{Δ8}			10~13 ^{Δ8}	14~19 ^{Δ8}	20 ^{Δ8}	Entropy requirement value (bit) ^{Δ4}	Key generation ^{Δ3}	_ ^{Δ3}	80 ^{Δ3}	80 ^{Δ3}	C&R authentication ^{Δ3}	The value shall be determined according to(*2) ^{Δ3Δ10}	The value shall be determined according to (*2) ^{Δ3Δ10}	The value shall be determined according to (*2) ^{Δ3Δ10}	Algorithm unpredictability requirement value	Key generation ^{Δ5}	Backward secrecy&Forward secrecy ^{Δ5}			C&R authentication ^{Δ5}	Forward secrecy(*4) ^{Δ5Δ13}		
	Random Number use case ^{Δ3Δ5}	Target AP ^{Δ8}																												
		10~13 ^{Δ8}	14~19 ^{Δ8}	20 ^{Δ8}																										
Entropy requirement value (bit) ^{Δ4}	Key generation ^{Δ3}	_ ^{Δ3}	80 ^{Δ3}	80 ^{Δ3}																										
	C&R authentication ^{Δ3}	The value shall be determined according to(*2) ^{Δ3Δ10}	The value shall be determined according to (*2) ^{Δ3Δ10}	The value shall be determined according to (*2) ^{Δ3Δ10}																										
Algorithm unpredictability requirement value	Key generation ^{Δ5}	Backward secrecy&Forward secrecy ^{Δ5}																												
	C&R authentication ^{Δ5}	Forward secrecy(*4) ^{Δ5Δ13}																												

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		35/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

	<p>Then</p> $H \geq \max_{1 \leq x \leq 24} \left\{ \log_2 \frac{365x(25-x)c}{T} + 1 \right\}$ <p>Ex.) When $T = 1\text{ms}$, $H \geq 51.7\text{bit}$ satisfies the above formula.</p> <p>If a penalty is necessary</p> <p>H: Entropy [bit]</p> <p>T: Processing time from C&R authentication challenge request to challenge response (average processing time at one time) [ms]</p> <p>T': Processing time from C&R authentication challenge request to challenge response (average processing time at one time including penalty time) [ms]</p> <p>N: Number of authentication failures before a penalty occurs [times]</p> <p>P: Weight time due to penalty [ms]</p> <p>c: Unit conversion coefficient ($1000 \times 60 \times 60 \times 24 \times 365$)</p> <p>Then</p> $H \geq \max_{1 \leq x \leq 24} \left\{ \log_2 \frac{365x(25-x)c}{T'} + 1 \right\}$ $T' = (N \cdot T + P) / N$ <p>Ex.) When $T = 1\text{ms}$ and $H = 40\text{bit}$, the above formula is satisfied with a penalty of $N \leq 3$ times and $P \geq 10$ seconds.^{Δ10}</p> <p>*3) For “Backward Secrecy” and “Forward Secrecy”, see KS2011 - DRG.2 equivalent to AIS20 - K3.^{Δ5}</p> <p>*4) For “Forward Secrecy”, see KS2011 - DRG.1^{Δ13}</p> <p>- Conduct design with the maximum required entropy value and algorithm unpredictability requirement value at the relevant Target AP^{Δ8} if the usage of the random number does not fall in the usages in the above-mentioned table.^{Δ3Δ5}</p> <p>- The department in charge of system (each design department), the department in charge of part (each design department), the department responsible for security (the department issuing this specifications) and the supplier shall discuss the possibility of addressing the issue with an alternative countermeasure requirement if the required entropy value and algorithm unpredictability requirement value is less than that described in the above-mentioned table.^{Δ3Δ5}</p> <p>- The designer shall confirm that the random number satisfies the requirements of KS2011 - DRG.2.4 with reference to the below-mentioned table in order to design the random number to be output with different values at a certain probability or more. If the cryptographic algorithm that satisfies the requirement of VULCMN_00100 is used, the requirement of</p>
--	---

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		36/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

	KS2011 - DRG.2.4 is satisfied. ^{Δ13Δ14}												
	<table border="1"> <thead> <tr> <th rowspan="2"></th><th colspan="3">Target AP</th></tr> <tr> <th>10~13 (AVA_VAN.2)</th><th>14~19 (AVA_VAN.3)</th><th>20 (AVA_VAN.4)</th></tr> </thead> <tbody> <tr> <td>Requirement for 128bit random number strings collision k: The number of 128bit random number strings ε: Collision probability</td><td>$k > 2^{14}$ and $\epsilon < 2^{-8}$</td><td>$k > 2^{19}$ and $\epsilon < 2^{-10}$</td><td>$k > 2^{26}$ and $\epsilon < 2^{-12}$</td></tr> </tbody> </table>				Target AP			10~13 (AVA_VAN.2)	14~19 (AVA_VAN.3)	20 (AVA_VAN.4)	Requirement for 128bit random number strings collision k: The number of 128bit random number strings ε: Collision probability	$k > 2^{14}$ and $\epsilon < 2^{-8}$	$k > 2^{19}$ and $\epsilon < 2^{-10}$
	Target AP												
	10~13 (AVA_VAN.2)	14~19 (AVA_VAN.3)	20 (AVA_VAN.4)										
Requirement for 128bit random number strings collision k: The number of 128bit random number strings ε: Collision probability	$k > 2^{14}$ and $\epsilon < 2^{-8}$	$k > 2^{19}$ and $\epsilon < 2^{-10}$	$k > 2^{26}$ and $\epsilon < 2^{-12}$										
	<p>(2): ^{Δ12 Δ13}</p> <p>The designer shall use pseudo random number generator complied with SP800-90A which is used entropy source output complied with SP800-90B as random number seed.</p> <p>And the pseudo random number generator shall be satisfied followings.</p> <p>- Security strength (*5): 128bit or more</p> <p>(Supplement) Pseudo random number generation algorithm (*5): The algorithm can be adopted one of the Hash_DRBG, HMAC_DRBG or CTR_DRBG. But, in case of CTR_DRBG, block cipher should be used AES.</p> <p>*5) Refer to SP800-90A about Security strength and Pseudo random number generation algorithm.</p>												
Reasons	<p>A low degree of randomness may increase the vulnerability of the authentication function. Random number generation is a prerequisite of security measures. It is used for all Target AP. ^{Δ13}</p> <p>However, because the necessary entropy and algorithm unpredictability requirement vary depending on the application and/or the threat, it is necessary to specify the target entropy for each product. ^{Δ5}</p> <p>If the product is equipped with hardware true random number generator, as long as the performance of the generator is adequate, use of this function ensures generation of random numbers with adequate randomness.</p> <p>365 in the above formula represents the number of correct combinations of challenges and responses available per year, and 25 represents the lifetime of the vehicle. ^{Δ10}</p>												

Attacks that cause generation of same random numbers shall be prevented.

ID	VULCMN_00300 ^{Δ6}	
Application	Functions/Parts	ECUs with random number generators ^{Δ7}

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		37/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

conditions ^{Δ6Δ12}	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		<p>When the random numbers given below are generated, do not use those numbers.</p> <ul style="list-style-type: none"> - ALL0 (All bits in the random number bit string are 0.)^{Δ4} - ALL1 (All bits in the random number bit string are 1.)^{Δ4} - Random numbers that match the previous random numbers (*) <p>(This requirement assumes attacks to random numbers in the field, not during the development phase.)</p> <p>*) After ECU reset, when the random number is first used, the following may avoid memorizing the random number before the reset. ^{Δ7}</p> <p>After resetting, the random number is generated twice in a row, and after confirming that the random number generated the second time is different from the random number generated the first time (the previous random number), the second generation random number is used. ^{Δ7}</p>
		<p>Attacks that cause generation of same random numbers generate the random numbers described above and they are no longer random.</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		38/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.2.2.2. Evaluation Requirements

ID		VULCMN_50200 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs with random number generators ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		<p>This requirement should be implemented when applying VULCMN_00200.</p> <p>When using a true random number generator, check that the generated numbers satisfy AIS31, and when using a pseudo random number generator, check that the generated numbers satisfy AIS20 using the randomness standard test. Or check that the pseudo random number generator and the entropy source constituting the random number generator are satisfied with criteria of SP800-90A and SP800-90B. ^{Δ12(*1)}^{Δ4}</p> <p>*1) When random number generator supplied from the vendor is used, either of the followings shall be performed.^{Δ4}</p> <ul style="list-style-type: none"> - Receive the result of the randomness standard test of AIS20, and AIS31 performed from the vendor.^{Δ4} Or receive the result of the randomness standard test of SP800-90A and SP800-90B performed. ^{Δ12} - Perform the randomness standard test of AIS20, and AIS31 for the random number generator.^{Δ4} (*2) Or perform the randomness standard test of SP800-90A and SP800-90B. ^{Δ12(*3)} <p>*2) Refer to KS2011 2.4.3. Standard Statistical Tests and 2.4.4. Test procedures for the method of conducting the randomness standard test.^{Δ7}</p> <p>If the designer choose with penalty in C&R authentication, the designer shall confirm that the penalty requirement is satisfied by functional test. ^{Δ10}</p> <p>*3) Refer to Test Vectors published by CAVP, SP800-90A 11.Assurance and SP800-90B 3.Entropy Source Validation chapter and later for the method of conducting the randomness standard test. ^{Δ12}</p>
Items to be checked		Randomness, Validity of the penalty countermeasure ^{Δ10}

ID		VULCMN_50300 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs with random number generators ^{Δ7}
	Target AP ^{Δ4Δ7}	All ^{Δ4Δ5Δ7}
Requirements		<p>This requirement should be implemented when applying VULCMN_00300.</p> <p>The countermeasure requirements shall be satisfied through functional tests.</p> <p>If functional tests are not feasible, perform verification by holding Design Review^{Δ4Δ6} of the functional specifications.</p>
Items to be checked		<p>Whether countermeasures are implemented</p> <p>Validity of countermeasures</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		39/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

4.3. Resistance to Closed Attacks on In-vehicle Parts

Closed attacks on in-vehicle parts are classified into those that exploit essential vulnerabilities of the function and those that exploit the privileged functions which permit direct access to memories in in-vehicle parts. Countermeasures and evaluation requirements for each attack are explained in the following sections.

4.3.1. Countermeasures for Privileged Functions of In-vehicle Parts without Opening (Debug, Maintenance)

4.3.1.1. Countermeasure Requirements

Attacks exploiting privileged functions that can be used without opening in-vehicle parts shall be prevented.^{Δ7}

ID		VULCMN_00400 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs to install privileged functions that can be used without opening in-vehicle parts ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		<p>When installing^{Δ2} privileged functions except the function permitted by the department responsible for security of Toyota Motor Coporation^{Δ2}, the privileged functions^{Δ4} shall be removed prior to the shipping of the product. (*1)^{Δ4}</p> <p>The privileged functions permitted by the department responsible for security are shown below. ^{Δ12}</p> <ul style="list-style-type: none"> -Standard Reprogramming Function -OTA Reprogramming Function^{Δ15} <p>But, about privileged functions that are not available via communication from global bus and that are used via wired I/F ^{Δ9} (the ones which are using connector pins inside the frames of the dotted lines on Fig. 4-1), remaining privileged functions are^{Δ4} acceptable if those^{Δ4} satisfy the requirements on “4.4.1Countermeasures for Privileged Functions of In-vehicle Parts by Opening (Test Access Port)”. ^{Δ2}</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure	40/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

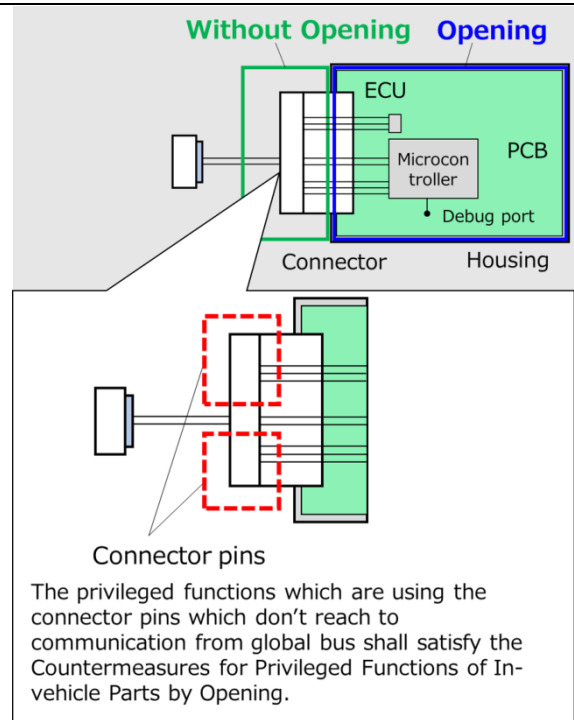


Fig. 4-1 Connector pins which don't reach to communication from global bus^{Δ2}

The due date for the countermeasures: By the product shipment on 1A at the latest, the countermeasures described shall be enabled. ^{Δ2}

If it is impossible to remove the privileged functions necessarily with the case except the above^{Δ2}, notify the department in charge of the security of Toyota Motor Corporation of the purpose of the privileged functions, security measures, etc. (*2) and obtain an agreement from them.

But, in cases that privileged functions of in-vehicle parts without opening are RR6 or less even if communication is spoofed from global bus and that protection measure requirements for CSPs/PSPs (VULCMN_01600 to VULCMN_01900^{Δ13}) are satisfied, remaining privileged functions are acceptable without above notification. ^{Δ12}

As a method of achieving RR6 or less, there is a method of prohibiting the operation of the privileged functions of the ECU by using the operation permission condition.

Ex) The operation permission condition of privileged functions are set vehicle

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		41/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

	<p>speed = 0km/h.</p> <p>But the signal which is using to operation permission condition shall be protected from spoofing by followings measures. ^{Δ12}</p> <ul style="list-style-type: none"> - Direct lines, Local communication lines, Message authentication^{Δ12} <p>*1) That the privileged functions shall be removed means removing of logics for the privileged functions. A case that removing of connectors as I/F of privileged functions from an in-vehicle part is performed not to enable to use the privileged functions, without removing of the logics, the connector is restored with opening the in-vehicle part, and the privileged functions have potentiality to be exploited. So the case shall satisfy the requirements on “4.4.1 Countermeasures for Privileged Functions of In-vehicle Parts by Opening (Test Access Port)” as well as unavailable privileged functions with communication from global bus. ^{Δ4}</p> <p>*2) Information regarding the privileged functions to be notified to the department in charge of security of Toyota Motor Corporation</p> <ul style="list-style-type: none"> - Names - Purposes - Applications - Risks due to presence of functions in field (assuming exploitation) - Security measures - Security evaluation specifications - Evaluation results <p>Promptly notify the department in charge of the security of Toyota Motor Corporation if it is impossible to remove the privileged functions. However, before notification, confirm that the prohibition condition on the privileged function is not defined, including specifications other than this document^{Δ5}</p> <p>E.g. Prohibition condition of ServiceID 0xBA of Phase5 Diagnosis^{Δ5}.</p>
Reasons	<p>If a privileged function to which security measures are not taken is implemented, adequate security measures taken on other privileged functions will not be any use.</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		42/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

Attacks exploiting privileged functions that can be used without opening in-vehicle parts shall be prevented (measures at gateways).

ID		VULCMN_00500 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs to install privileged functions that can be used without opening in-vehicle parts ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		<p>To prevent the privileged functions that can be used without opening the in-vehicle parts placed with a permission obtained by the department in charge of the security^{Δ4} from being exploited (*1), disable them prior to the shipping or use access control. Password authentication or C&R authentication shall be used to control accesses.</p> <ul style="list-style-type: none"> - The password length shall be 128 bits or more. ^{Δ6} - The password set by string shall contain at least numbers, uppercase letters and lowercase letters, and shall be at least 8 digits in length. ^{Δ9} - The encryption key used for C&R authentication shall be 128 bits or more. - The encryption algorithm used for C & R authentication shall meet the requirements of VULCMN_00100, and the random numbers shall meet the requirements of VULCMN_00200 and VULCMN_00300. ^{Δ2Δ6} <p>If countermeasure requirements regarding the access control of the privileged functions that can be used without opening the in-vehicle parts more detailed than this document are given in the documents (*4), follow those descriptions.</p> <p>*1) Posing threats (*2) to information assets including CSPs^{Δ4}, safety, corporate assets, privacy, etc.</p> <p>*2) Example threats to information assets are:</p> <ul style="list-style-type: none"> - CSP: Leakage of CSPs^{Δ4} - Safety: Tampering of controls and programs of risk level 7 or higher - Corporate assets: Leakage of programs - Privacy: Leakage of personal and privacy information (*3) <p>*3) For personal and privacy information, see “Standards of Personal and Privacy Information” and “Requirements of Personal and Privacy Information”.</p> <p>*4) “Constitution of Diagnostics”^{Δ2}, “Requirements Specification of Standard Reprogramming Security”, etc. ^{Δ1}</p>
Reasons		To prevent exploitation of privileged functions.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		43/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

ID	VULCMN_00501 ^{Δ6}	Application conditions ^{Δ6Δ12}	Functions/Parts	When disabling privileged functions is adopted in VULCMN_00500 ^{Δ7}
			Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
		When the privileged function which can be used without opening the in-vehicle part will not be used after the shipping of the product, it shall be disabled.		
ID	VULCMN_00502 ^{Δ6}	Application conditions ^{Δ6Δ12}	Functions/Parts	When VULCMN_00500 adopts access control to privileged functions ^{Δ7}
			Target AP ^{Δ7}	10~13 ^{Δ7}
		When the privileged function which can be used without opening the in-vehicle part will be used after the shipping of the product, its access shall be controlled. As the access control means, password authentication or C&R authentication shall be used. The confidential information to be used for authentication (password, encryption key) may be shared among the same part no.		
ID	VULCMN_00503 ^{Δ6}	Application conditions ^{Δ6Δ12}	Functions/Parts	When VULCMN_00500 adopts access control to privileged functions ^{Δ7}
			Target AP ^{Δ7}	14~20 ^{Δ7}
		When the privileged function which can be used without opening the in-vehicle part will be used after the shipping of the product, its access shall be controlled. As the access control means, password authentication or C&R authentication shall be used. The confidential information used for authentication (password, encryption key) shall not affect other vehicles in case of leakage. E.g. - Separate password or encryption key for the C&R authentication shall be established for each in-vehicle part (each serial no.). - Alternatively, use a public key.		

ID		VULCMN_00600 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	-
	Target AP ^{Δ7}	-
Requirements		Deleted.
Reasons		-

ID		VULCMN_00700 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	When VULCMN_00500 adopts access control to privileged functions
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		44/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

Requirements	Even in the state where the authentication in VULCMN_00500 has been completed successfully (authenticated state), when the in-vehicle part is reset, the part shall switch back to the previous state (unauthenticated state). E.g. IG-OFF to IG-ON operation during the authenticated state cancels the authenticated state.
Reasons	If the vehicle is returned to the user while the in-vehicle part is in the “authenticated state”, the user can potentially use the privileged function.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		45/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

Attacks exploiting privileged functions that can be used without opening in-vehicle parts shall be prevented (internal countermeasures).

ID		VULCMN_00800 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	When VULCMN_00500 adopts access control to privileged functions
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		<p>Even after the authentication in VULCMN_00500, only the data necessary for the applicable privileged function shall be made accessible.</p> <p>(Supplement)</p> <p>This requirement demands that data accessible by privileged functions be exactly defined. For example, after passing the authentication for diagnostics purposes but before passing the authentication for reprogramming purposes, the data to be used by the reprogramming function is not made accessible. ^{Δ13}</p>
Reasons		<p>If the function for checking some control parameters is capable of reading encryption keys, parties who are not entitled to know encryption keys have access to the encryption keys. Important parameters such as encryption keys that relate to the fundamentals of the security need to be closely controlled.</p> <p>Therefore, it is necessary to clarify the items that should not be read and perform access control appropriate for the purpose.</p>

ID		VULCMN_00900 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	When VULCMN_00500 adopts access control to privileged functions
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		<p>Even before the authentication in VULCMN_00500, the data that can be accessed by all parties shall be clarified and access shall be permitted to those data only.</p> <p>(Supplement)</p> <p>This requirement requires that data accessible by any party be defined. For example, when reading is required by a law, etc., it is required that only necessary data can be read in a white list format.</p>
Reasons		In relation to VULCMN_00800, items that are to be read need to be clearly defined.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		46/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.3.1.2. Evaluation Requirements

ID		VULCMN_50400 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	VULCMN_00400, VULCMN_00500, VULCMN_00501, VULCMN_00502, VULCMN_00503, VULCMN_00800, VULCMN_00900. When even one of the above requirements is applied. ^{Δ7}
	Target AP ^{Δ7}	According to the target AP of the corresponding countermeasure requirements. ^{Δ4Δ5Δ7}
Requirements		Check that the debug/maintenance functions connected to the backdoor are limited to the scope agreed with Toyota Motor Corporation.
Items to be checked		Whether backdoors exist Validity of maintenance modes

ID		VULCMN_50500 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	VULCMN_00500, VULCMN_00501, VULCMN_00502, VULCMN_00503, VULCMN_00700, VULCMN_00800, VULCMN_00900. When even one of the above requirements is applied. ^{Δ7}
	Target AP ^{Δ7}	According to the Target AP of the corresponding countermeasure requirements. ^{Δ4Δ5Δ7}
Requirements		The countermeasure requirements shall be satisfied through functional tests.
Items to be checked		Whether countermeasures are implemented Validity of the countermeasures

4.3.2. Countermeasures in Specifications

4.3.2.1. Countermeasure Requirements

Attacks exploiting vulnerabilities created in the specification definition stage shall be prevented.

ID		VULCMN_01000 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	All ECUs ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		The ECU shall not install functions (concealed function) for specifications not specified by Toyota Motor Corporation.(*) ^{Δ1Δ14} *) Does not include disabling functions. ^{Δ14} If off-the-shelf products already install functions (concealed function) for specifications not specified by Toyota Motor Corporation, logics for the functions shall be removed. ^{Δ14}

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		47/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

	<p>If it is unavoidable to install functions (concealed function) for specifications not specified by Toyota Motor Corporation in the ECU, the functions shall satisfy the security requirements and obtain an agreement from the department in charge of system (each design department) and the department in charge of part (each design department). ^{Δ14}</p> <p>E.g. Software used during only the development phase, inspection software, and other unnecessary software shall not be installed in production parts.</p>
Reasons	<p>If a function that has not been approved by Toyota Motor Corporation and that may lead to backdoor remains in the market product, it can be used by attackers to access data that are normally not available to them. Excess functions may be potentially exploited by attackers.</p>

ID		VULCMN_01100 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	All ECUs ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		<p>Clarify the I/F(*)^{Δ4} specifications of the boundaries between the in-vehicle parts and</p> <ul style="list-style-type: none"> - do not operate in reaction to any input outside the scope of specification - do not make any output outside the scope of specification <p>*) A case that an in-vehicle part can be connected to other parts via connectors and wireless, this requirement shall be applied to the case. ^{Δ4}</p> <p>E.g. Abnormal operation is not made even though the actual data length does not match the specified data length during a diagnostics or the like. ^{Δ13} (Anomaly process is carried out.) ^{Δ1Δ13}</p>
Reasons		<p>There are attacks that involve making abnormal inputs and observing the behavior to analyze the processing and that involve causing abnormal operations and making outputs outside the scope of specification.</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		48/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.3.2.2. Evaluation Requirements

ID		VULCMN_50600 ^{Δ6}
Application	Functions/Parts	All ECUs ^{Δ7}
conditions ^{Δ6Δ12}	Target AP ^{Δ4Δ7}	All ^{Δ4Δ5Δ7}
Requirements		<p>This requirement should be implemented when applying VULCMN_01000.</p> <p>The ECU designer shall confirm whether or not a function that does not correspond to Specifications specified by Toyota Motor Corporation are installed.^{Δ6Δ12 Δ16}</p> <p>If it is unavoidable to install functions for specifications not specified by Toyota Motor Corporation in the ECU, the ECU designer shall confirm that the functions satisfy the security requirements and the ECU designer obtained an agreement from Toyota Motor Corporation.</p> <p>^{Δ16}</p>
Items to be checked		<p>(1) Whether correspondence relationship between Specifications specified by Toyota Motor Corporation and function implemented on matrix table is indicated.</p> <p>(2) Whether function for specifications not specified by Toyota Motor Corporation are not included.</p> <p>(3) If it is unavoidable to install functions for specifications not specified by Toyota Motor Corporation, validity of the functions.^{Δ16}</p> <p>(4) Whether table of review results regarding the correspondence relationship is described.</p>

ID		VULCMN_50700 ^{Δ6}
Application	Functions/Parts	All ECUs ^{Δ7}
conditions ^{Δ6Δ12}	Target AP ^{Δ4Δ7}	All ^{Δ4Δ5Δ7}
Requirements		<p>This requirement should be implemented when applying VULCMN_01100.</p> <p>The countermeasure requirements shall be satisfied through functional tests.</p>
Items to be checked		<p>Whether countermeasures are implemented</p> <p>Validity of countermeasures</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		49/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.3.3. Secure Coding

4.3.3.1. Countermeasure Requirements

Attacks exploiting coding-related vulnerabilities shall be prevented.

ID		VULCMN_01200 ^{Δ6}										
Application	Functions/Parts	All ECUs ^{Δ7}										
conditions ^{Δ6Δ12}	Target AP ^{Δ7}	All ^{Δ4Δ5Δ6Δ7}										
Requirements		<p>To reduce vulnerabilities of software, ^{Δ5} for all software in ECU, the coding rules given below shall be applied^{Δ16}.</p> <ul style="list-style-type: none"> - C language: MISRA-C and CERT-C shall be applied in accordance with ^{Δ13} TSC7030G (C language coding standard for software embedded in in-vehicle electric/electronic parts). - C++ language: MISRA-C ++, AUTOSAR C ++ 14 and CERT-C ++ shall be applied in accordance with ^{Δ13} TSC7047G (C++ language coding standard for software embedded in in-vehicle electric/electronic parts). - Languages other than C language, and C++ language^{Δ4}: Secure coding rules appropriate for each language shall be complied. <p>E.g. ISO/IEC TR 24772, CERT-JAVA, CERT-Perl</p> <p>And, the legacy^{Δ4} software, the automatically generated code of model-based development and the external procurement software shall support secure coding in the following table.^{Δ16}</p> <table> <tr> <th>Software types</th><th>Execution contents(either one)</th><th>In case that it is difficult to support secure coding</th></tr> <tr> <td>Legacy software</td><td rowspan="2">- Comply with secure coding rules (*1)</td><td rowspan="2">Contact to the department in charge of the security (issuing dept. of this document) and get agreement</td></tr> <tr> <td>Automatically generated code of model-based development</td></tr> <tr> <td>External procurement software</td><td> <ul style="list-style-type: none"> - Use secure coding supported software - Comply with secure coding rules (*1) </td><td>Do vulnerability analysis and risk treatment (retention/avoidance/sharing/reduction)</td></tr> </table> <p>*1) You may check the codes using a static program analysis tool that enables secure coding checks(*2), and then fix only deviations from the coding rule that are not acceptable from security perspectives(*3).</p>	Software types	Execution contents(either one)	In case that it is difficult to support secure coding	Legacy software	- Comply with secure coding rules (*1)	Contact to the department in charge of the security (issuing dept. of this document) and get agreement	Automatically generated code of model-based development	External procurement software	<ul style="list-style-type: none"> - Use secure coding supported software - Comply with secure coding rules (*1) 	Do vulnerability analysis and risk treatment (retention/avoidance/sharing/reduction)
Software types	Execution contents(either one)	In case that it is difficult to support secure coding										
Legacy software	- Comply with secure coding rules (*1)	Contact to the department in charge of the security (issuing dept. of this document) and get agreement										
Automatically generated code of model-based development												
External procurement software	<ul style="list-style-type: none"> - Use secure coding supported software - Comply with secure coding rules (*1) 	Do vulnerability analysis and risk treatment (retention/avoidance/sharing/reduction)										

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		50/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

	<p>*2) Receiving the verification result from a software vendor and confirming the result are acceptable.^{Δ5}</p> <p>*3) Confirm posing threats (*4) to information assets including CSPs, safety, corporate assets, privacy, etc. ^{Δ5}</p> <p>*4) Example threats to information assets are: ^{Δ5}</p> <ul style="list-style-type: none"> - CSP: Leakage of CSPs^{Δ5} - Safety: Tampering of controls and programs of risk level 7 or higher^{Δ5} - Corporate assets: Leakage of programs^{Δ5} - Privacy: Leakage of personal and privacy information (*5) ^{Δ5} <p>*5) For personal and privacy information, see “Standards of Personal and Privacy Information” and “Requirements of Personal and Privacy Information”. ^{Δ5}</p> <p>Discuss whether measures are necessary among the department in charge of the system (each design department), the department in charge of the part (each design department), the department in charge of the coding (PQF^{Δ5}), the department in charge of the security (issuing dept. of this document), and the supplier.</p>
Reasons	Reduce vulnerabilities by performing coding in accordance with the rules.

Prevent the program from being analyzed (ROM on PCB, programs in microcontroller).

ID	VULCMN_01300 ^{Δ6}	
Application conditions ^{Δ6Δ12}	Functions/Parts	All ECUs ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ6Δ7}
Requirements	<p>Do not write a list of symbols to the ROM on the PCB or the flash memory in the microcontroller of the in-vehicle part (except the prototype phase).</p> <p>* When the programming language is C or C++</p>	
Reasons	<p>If the list of the symbols is kept in the in-vehicle part in the market, it may be analyzed and exploited (*). Therefore, it is necessary to eliminate it.^{Δ7}</p> <p>*) See (*1) of VULCMN_00500.</p>	

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		51/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.3.3.2. Evaluation Requirements

ID		VULCMN_50800 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	All ECUs ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		<p>The software shall be compliant with each programming language coding rules with in VULCMN_01200. ^{Δ16}</p> <p>The legacy software and the automatically generated code shall be compliant with secure coding rules.</p> <p>If confirming compliant with the secure coding rules with using static code analysis tools, “Recommended tools” column shall be referred.</p> <p>If there are items cannot be checked by the static code analysis tool, countermeasure requirement shall be satisfied with source code review. ^{Δ16}</p> <p>The external procurement software shall be compliant with corresponding to secure coding. If secure coding is not supported, it shall be compliant with corresponding to risk treatment. ^{Δ16}</p> <p>If there is a violation of the rule, the reason for the violation shall be permissible in terms of security. ^{Δ12}</p>
Recommended tools		Klocwork, Coverity, CodeSonar, QA・C, LDRA, Fortify SCA (use of the latest version is recommended)
Items to be checked		Whether vulnerabilities exist in implementation

ID		VULCMN_50900 ^{Δ6Δ16}
Application conditions ^{Δ6Δ12}	Functions/Parts	-
	Target AP ^{Δ7}	-
Requirements		(Deleted)
Items to be checked		-

ID		VULCMN_51000 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	All ECUs ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ6Δ7}
Requirements		<p>This requirement should be implemented when applying VULCMN_01300.</p> <p>Symbol shall not be included in the binary for writing dumped.</p>
Items to be checked		Whether symbol is not included in the binary of writing.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		52/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

4.3.4. Protection Measures for Programs/Data (Protection of Programs)

4.3.4.1. Countermeasure Requirements

Attacks involving tampering of the program shall be prevented (program inside the microcontroller).

ID		VULCMN_01400 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs with reprogramming function ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		Programs received from outside the in-vehicle part shall be run after checking its integrity. E.g. At the time of reprogramming, check the integrity of the received program and store the flags, and perform flag check only at the following boot.
Reasons		In-vehicle parts with the reprogramming function should be capable of checking the validity of the written program and preventing operations on invalid programs. ^{Δ13} This must be ensured by the in-vehicle parts having the reprogramming function.

ID		VULCMN_01500 ^{Δ6Δ12}
Application conditions ^{Δ6Δ12}	Functions/Parts	
	Target AP ^{Δ7}	
Requirements		Deleted.
Reasons		

4.3.4.2. Evaluation Requirements

ID		VULCMN_51100 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	VULCMN_01400 is applied. ^{Δ7Δ12}
	Target AP ^{Δ7}	According to the target AP of the corresponding countermeasure requirements. ^{Δ4Δ5Δ7}
Requirements		The countermeasure requirements shall be satisfied through functional tests.
Items to be checked		Whether countermeasures are implemented Validity of countermeasures

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		53/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.3.5. Protection Measures for Programs/Data (Protection of CSPs ・ PSPs)

4.3.5.1. Countermeasure Requirements

Attacks involving leakage and tampering of CSPs shall be prevented / Attacks involving tampering of PSPs shall be prevented

ID		VULCMN_01600 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs that use and store passwords ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		<p>Following requirements for (1) or (2) shall be satisfied. ^{Δ13}</p> <p>(1) For password, it shall be satisfied with protection requirements of CSP which are VULCMN_01700, VULCMN_01701 and VULCMN_01702. ^{Δ13}</p> <p>(2) For password, it shall change to hash value and be stored in memory. The hash value shall be satisfied with protection requirements of PSP which are VULCMN_01700, VULCMN_01701 and VULCMN_01702 because the password which is changed to hash value is PSP. ^{Δ13}</p>
Reasons		It is necessary to store passwords in a format which cannot be used in case they are read.

ID		VULCMN_01700 ^{Δ6}		
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs that store CSPs / PSPs ^{Δ7}		
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}		
Requirements		<p>CSPs shall be stored in secured memory (*).</p> <p>*) Secured memory</p> <ul style="list-style-type: none"> - Memory with limited access from outside (“Read” and “Write”) - Memory which permits access to specific tasks^{Δ13} - Memory which can be accessed by only directly processing unit in HSM^{Δ13} <p>If the protected data is PSP, store it in memory with limited “Write” (“Read” may not be limited, storing in memory which can be accessed by only directly processing unit in HSM is not required). ^{Δ7}</p>		
Reasons		<p>It is necessary that CSPs are stored in a memory with at least limited access (“Read” and “Write”) from outside (privileged functions such as diagnostics function, JTAG and other microcontroller-level privileged functions) (For PSPs, “Write” restrictions.^{Δ7}). When assuming higher-level attacks such as software hijacking, it is also necessary to limit access from the CPU.</p>		
ID	VULCMN_01701 ^{Δ6}	Application	Functions/Parts	ECUs that store CSPs / PSPs ^{Δ4Δ5Δ7}

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		54/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

		conditions ^{Δ6Δ12}	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
		<p>When storing CSPs in a memory of the microcontroller, access from outside (“Read”and“Write”) shall be limited to prevent direct reading and writing from outside.</p> <p>The design shall permit read and write of specific functions only.</p> <p>When storing PSPs in a memory of the microcontroller, “Write” from outside shall be limited. ^{Δ14}</p> <p>(Read may not be restricted.) ^{Δ7}</p> <p>When storing the CSPs in the external memory of the microcontroller necessarily, encrypt them and carry out tampering detection (signature verification)^{Δ4} for them.^{Δ2}</p> <p>When storing PSPs in the external memory of the microcontroller necessarily, tampering detection for them shall be implemented. ^{Δ14}</p> <p>(Encryption may not be implemented) ^{Δ7}</p> <p>- AP10~13^{Δ7} : The encryption keys to be used for encryption and tampering detection may be shared among the same part no.^{Δ2}</p> <p>- AP14~20^{Δ7} : The encryption keys to be used for encryption and tampering detection don’t affect other vehicles in case of leakage.^{Δ2}</p> <p>Protection of the above encryption keys to be used for encryption or tampering detection shall be satisfied requirement VULCMN_01702. ^{Δ10Δ13}</p> <p>E.g. ^{Δ2}</p> <p>- Separate encryption key is established for each in-vehicle part (each serial no.). ^{Δ2}</p> <p>- Alternatively, use a public key. ^{Δ2}</p>		
ID	VULCMN_01702 ^{Δ1Δ6}	Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs that store CSPs / PSPs ^{Δ7Δ10}
			Target AP ^{Δ7}	14~20 ^{Δ4Δ5Δ7Δ10}
		<p>The ECU shall have HSM^{Δ13}, and only the processing unit in HSM^{Δ13} shall be able to access CSPs and PSPs directly.</p> <p>However, session keys for the purpose of processing the generation, updating, and using CSP are excluded from this requirement and shall satisfy VULCMN_01701.</p> <p>In that case, the CSP shall be deleted from the memory immediately after the processing is completed. ^{Δ13}</p> <p>Example of deleting) Overwrite the CSP in the memory with zero. ^{Δ13}</p>		

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		55/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

		<p>When storing PSPs in a memory of the microcontroller necessarily, “Write” from outside shall be limited by using hardware function. ^{Δ14}</p> <p>When storing PSPs in the external memory of the microcontroller necessarily, PSPs shall be stored in a tamper-detectable state (MAC or signed state) in memory.^{Δ7} In addition, only the processing unit in HSM shall be able to access the key to be used for tampering detection directly.</p>
--	--	---

ID		VULCMN_01800 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs that distribute CSPs / PSPs ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		<p>When distributing the CSP to other in-vehicle parts, it shall be distributed while maintaining its confidentiality and integrity.</p> <p>If the protected data is PSP, distribute it with integrity.</p> <p>(Confidentiality may not be ensured.) ^{Δ7}</p> <p>E.g. Utilization of shared key protocol, information dispersion</p>
Reasons		When distributing a CSP or PSP, it is necessary to maintain the confidentiality and integrity with use of encryption or MAC to prevent the CSPs ^{Δ4} from being leaked or tampered(For PSPs, to prevent tampering).

ID		VULCMN_01900 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs that store CSPs / PSPs ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		When the update process is stopped due to power interruption, etc., the state prior to the update shall be able to be retained.
Reasons		If the CSP/PSP ^{Δ7} has some random value due to the interruption of the update process, the security function itself does not serve its purpose. Therefore, it is necessary that the value returns to that prior to the update process.

ID		VULCMN_02000 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	
	Target AP ^{Δ7}	
Requirements		Deleted ^{Δ13} .
Reasons		

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		56/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

4.3.5.2. Evaluation Requirements

ID		VULCMN_51200 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	VULCMN_01600, VULCMN_01700, VULCMN_01701, VULCMN_01702, VULCMN_01800, VULCMN_01900. When even one of the above requirements is applied. ^{Δ7}
	Target AP ^{Δ7}	According to the target AP of the corresponding countermeasure requirements. ^{Δ4Δ5Δ7}
Requirements		The countermeasure requirements shall be satisfied through functional tests.
Items to be checked		Whether countermeasures are implemented Validity of countermeasures

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		57/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.3.6. Protection Measures for Programs and Data (Protection of Data for Information-related In-vehicle Parts)

4.3.6.1. Countermeasure Requirements

Attacks involving leaking or tampering information-related data shall be prevented.

ID		VULCMN_02100 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs with TCP or UDP ports ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements ^{Δ14}		<ul style="list-style-type: none"> • In the case of TCP or UDP ports at the entry point, the ECU shall close the TCP/UDP ports not to be used. The ECU shall open the TCP/UDP ports to be used when the service starts or the ECU requests connection establishment, and the ECU shall close the port when the service finishes or the ECU terminates connection. • In the case of TCP or UDP ports other than the entry point, the ECU shall close the TCP/UDP ports not to be used.
Reasons		Unnecessary open ports can be potentially exploited for external attacks.

ID		VULCMN_02200 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs that use an OS with a file system ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		<p>The default access right for files and directories (permission) shall be set to “read only”.</p> <p>If operations other than read (write, execute, etc.) are necessary, their target files and directories and the users who are allowed to perform those operations (owner, users who belong to the owner group, other users, all users, etc.) shall be clarified.</p>
Reasons		The access right to files and directories should be limited to a minimum. ^{Δ6}

ID		VULCMN_02300 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs that can use multiple CPU modes ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		Privileged mode and user mode shall be separately defined exactly and data accessible in each mode shall be clarified.
Reasons		It is necessary to implement access right control with use of OS/OSS functions.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		58/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

ID		VULCMN_02400 ^{Δ6Δ12}
Application conditions ^{Δ6Δ12}	Functions/Parts	
	Target AP ^{Δ8}	
Requirements		Deleted.
Reasons		

ID		VULCMN_03700 ^{Δ9Δ10}
Application conditions ^{Δ12}	Functions/Parts	ECUs with the function to install 3rdParty applications (*1) or application that cannot satisfy security requirements (*2) ^{Δ10} *1) An application that Toyota is not involved in development. “Not involved” means not based on a development contract with Toyota. ^{Δ10} *2) An application that has been agreed with the department in charge of system (each design department), the department in charge of part (each design department), the department responsible for security (the department issuing this specifications) that the assigned security requirements cannot be satisfied. ^{Δ10}
	Target AP	14~20
Requirements		The entry point area where the 3rd Party applications or application that cannot satisfy security requirements ^{Δ10} are located shall satisfy the following requirements: <ul style="list-style-type: none"> • The data output from the 3rd Party applications or application that cannot satisfy security requirements^{Δ10} shall not affect the control of risk rank 7 or higher. • The access right (Read / Write / Execute) to the data / functions given to the 3rd Party application or application that cannot satisfy security requirements^{Δ10} by the OS shall limit to the data / functions permitted by the user.
Reasons		To minimize the risk of malware being installed and executed unintentionally.

ID		VULCMN_03800 ^{Δ9}
Application conditions ^{Δ12}	Functions/Parts	ECUs that use an OS with the login function
	Target AP	All
Requirements		The ECU shall prohibit direct login using root user, and shall restrict privilege escalation for general user.
Reasons		Root user is privileged authority. Because of the high risk of system abuse, it is necessary to operate with users who have been granted individual minimum necessary privileges.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		59/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

ID		VULCMN_03900 ^{Δ10}
Application conditions ^{Δ12}	Functions/Parts	ECUs that use an OS with the login function
	Target AP	All
Requirements		The password that is set to login to the OS shall contain at least numbers, uppercase letters and lowercase letters, and shall be at least 8 digits in length.
Reasons		The OS could potentially permit an unauthorized login by Brute Force Attack etc. if an insecure password is set.

ID		VULCMN_04000 ^{Δ10}
Application conditions ^{Δ12}	Functions/Parts	Applications with the password authentication function
	Target AP	All
Requirements		The password that is used by the applications shall contain at least numbers, uppercase letters and lowercase letters, and shall be at least 8 digits in length, or when the customer changes to a password which does not satisfy the above password requirement, the ECU shall notify the risk of it.
Reasons		The application could be potentially permit an unauthorized use by Brute Force Attack etc. if an insecure password is set. If it is difficult to be set a sufficient secure password, the application encourages an appropriate use by providing the attention for the customer.

4.3.6.2. Evaluation Requirements

ID		VULCMN_51300 ^{Δ6}
Application conditions ^{Δ12}	Functions/Parts	ECUs with TCP or UDP ports
	Target AP ^{Δ7}	All ^{Δ7}
Requirements		This requirement should be implemented when applying VULCMN_02100. The countermeasure requirements shall be satisfied through design verification.
Items to be checked		Check the following items for the validity of the countermeasures. <Countermeasure validity check items> - Name of the specification corresponding to the open port - Port no. - Service name - Overview - Purpose - Applications - Implementation of security measures when the port is open - Risks with port/service (when it is exploited)

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		60/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

	<ul style="list-style-type: none"> - Security measures - Security evaluation specifications - Evaluation result
--	--

ID		VULCMN_51400 ^{Δ6}
Application conditions ^{Δ12}	Functions/Parts	VULCMN_02200, VULCMN_02300. When either is applied. ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		The countermeasure requirements shall be satisfied based on the environment settings of OS and OSS ^{Δ1} .
Items to be checked		<p>Validity of the countermeasures</p> <p>Check the items below to examine the validity of the countermeasures.</p> <p><Countermeasure validity check items></p> <ul style="list-style-type: none"> - Name of file/directory - Overview - Purpose - Applications - Implementation of countermeasures - Risks of the access right owner and target user - Security measures - Security evaluation specifications - Evaluation result

ID		VULCMN_51500 ^{Δ6Δ12}
Application conditions ^{Δ12}	Functions/Parts	
	Target AP ^{Δ8}	
Requirements		Deleted.
Items to be checked		

ID		VULCMN_52600 ^{Δ9}
Application conditions ^{Δ12}	Functions/Parts	ECUs with function to install 3rdParty applications or application that cannot satisfy security requirements ^{Δ10}
	Target AP	14~20
Requirements		<p>This requirement should be implemented when applying VULCMN_03700.</p> <p>The countermeasure requirements shall be satisfied through design verification.</p>

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		61/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

Items to be checked	Whether countermeasures are implemented
	Validity of the countermeasures

ID		VULCMN_52700 ^{Δ9}
Application conditions ^{Δ12}	Functions/Parts	ECUs that use an OS with the login function
	Target AP	All
Requirements		This requirement should be implemented when applying VULCMN_03800. The countermeasure requirements shall be satisfied through functional test.
Items to be checked	Whether countermeasures are implemented	
	Validity of the countermeasures	

ID		VULCMN_52800 ^{Δ10}
Application conditions ^{Δ12}	Functions/Parts	ECUs that use an OS with the login function
	Target AP	All
Requirements		This requirement should be implemented when applying VULCMN_03900. The countermeasure requirements shall be satisfied through functional test.
Items to be checked	Whether countermeasures are implemented	
	Validity of the countermeasures	

ID		VULCMN_52900 ^{Δ10}
Application conditions ^{Δ12}	Functions/Parts	Applications with the password authentication function
	Target AP	All
Requirements		This requirement should be implemented when applying VULCMN_04000. The countermeasure requirements shall be satisfied through functional test.
Items to be checked	Whether countermeasures are implemented	
	Validity of the countermeasures	

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		62/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.4. Resistance to Open Attacks on In-vehicle Parts

Countermeasures against attacks involving opening and physically accessing the in-vehicle part and analyzing and tampering the data/programs are described in the following sections.

4.4.1. Countermeasures for Privileged Functions of In-vehicle Parts by Opening (Test Access Port)

4.4.1.1. Countermeasure Requirements

Attacks exploiting the privileged function which can be used by opening the in-vehicle part shall be prevented.

ID		VULCMN_02500 ^{Δ6}		
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs to install privileged functions that can be used with opening in-vehicle parts ^{Δ7}		
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}		
Requirements		<p>To prevent the privileged function (test access port) which can be used by opening the in-vehicle part from being exploited, the function shall be disabled prior to the shipping of the product or access control shall be implemented.</p> <p>As the access control means, password authentication or C&R authentication shall be used.</p> <ul style="list-style-type: none"> - The password length shall be 128 bits or more. ^{Δ6} - The password set by string shall contain at least numbers, uppercase letters and lowercase letters, and shall be at least 8 digits in length. ^{Δ9} - The encryption key used for C&R authentication shall be 128 bits or more. - The encryption algorithm used for C&R authentication shall meet the requirements of VULCMN_00100, and the random numbers shall meet the requirements of VULCMN_00200 and VULCMN_00300. ^{Δ2Δ6} <p>The due date for the countermeasures: By the product shipment on 1A at the latest, the countermeasures described^{Δ5} shall be enabled. ^{Δ2}</p>		
Reasons		When using privileged functions, it is necessary to prevent exploitations with use of authentication.		
ID	VULCMN_02501	Application conditions ^{Δ6Δ12}	Functions/Parts	When disabling privileged functions is adopted in VULCMN_02500 ^{Δ7}

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		63/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

			Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
		When the privileged function which can be used by opening the in-vehicle part will not be used after the shipping of the product, it shall be disabled.		
ID	VULCMN_02502	Application conditions ^{Δ6Δ12}	Functions/Parts	When VULCMN_02500 adopts access control to privileged functions ^{Δ7}
			Target AP ^{Δ7}	10~13 ^{Δ4Δ7}
		When the privileged function which can be used by opening the in-vehicle part will be used after the shipping of the product, access control shall be implemented for it. ^{Δ4} As the access control means, password authentication or C&R authentication shall be used. The confidential information to be used for authentication (password, encryption key) may be shared among the same part no.		
ID	VULCMN_02503	Application conditions ^{Δ6Δ12}	Functions/Parts	When VULCMN_02500 adopts access control to privileged functions ^{Δ7}
			Target AP ^{Δ7}	14~20 ^{Δ4Δ5Δ7}
		When the privileged function which can be used by opening the in-vehicle part will be used after the shipping of the product, access control shall be implemented for it. ^{Δ4} As the access control means, password authentication or C&R authentication shall be used. The confidential information to be used for authentication (password, encryption key) shall be designed so as not to affect other vehicles in case of leakage. E.g. - Separate password or an encryption key for C&R authentication is established for each in-vehicle part (each serial no.). ^{Δ13} - Alternatively, use a public key.		

ID		VULCMN_02600 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	When VULCMN_02500 adopts access control to privileged functions ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		Protected memory, CSPs ^{Δ4} shall not be read via the privileged function which can be used by opening the in-vehicle part. Take measures for VULCMN_02601 and VULCMN_02602. ^{Δ7}
Reasons		It is more secure to prohibit reading of encryption keys, etc. at the time of analysis failure. Indirect verification will be required such as verification using encryption result or the like.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		64/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

ID	VULCMN_02601 ^{Δ7}	Application conditions ^{Δ12}	Functions/Parts	Memory permission management features are available
			Target AP	All
		Read to the memory protected from privileged functions and CSP shall be prohibited by using the memory access right management function.		
ID	VULCMN_02602 ^{Δ7}	Application conditions ^{Δ12}	Functions/Parts	All ECUs
			Target AP	14~20
		The CSP shall be stored in a secure area where the bus is separated from the privileged functions available by opening the in-vehicle components. And make sure that only the processing unit in HSM ^{Δ13} can access the CSP.		

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		65/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.4.1.2. Evaluation Requirements

ID		VULCMN_51600 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	VULCMN_02500, VULCMN_02501, VULCMN_02502, VULCMN_02503, VULCMN_02600. When even one of the above requirements is applied. ^{Δ7}
	Target AP ^{Δ7}	According to the target AP of the corresponding countermeasure requirements. ^{Δ4Δ5Δ7}
Requirements		The countermeasure requirements shall be satisfied through functional tests.
Items to be checked		Whether countermeasures are implemented Validity of countermeasures

ID		VULCMN_51700 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	VULCMN_02500, VULCMN_02501, VULCMN_02502, VULCMN_02503, VULCMN_02600. When even one of the above requirements is applied. ^{Δ7}
	Target AP ^{Δ4Δ7}	According to the target AP of the corresponding countermeasure requirements. ^{Δ4Δ5Δ7}
Requirements		It shall be verified that the ranges of the debug/maintenance function connected to backdoors are limited to risk-free ranges.
Items to be checked		Whether backdoors exist Validity of maintenance modes

4.4.2. Countermeasures against PCB Analysis

4.4.2.1. Countermeasure Requirements

Analysis of confidential information exchanged between chips shall be prevented.

ID		VULCMN_02700 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs that communicate between microcontroller on in-vehicle parts / communicate between the microcontroller and external memory ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ4Δ5Δ7}
Requirements		When communication between the microcontrollers of the in-vehicle part and the microcontroller and an external memory contain CSPs ^{Δ4} use encryption to prevent analysis of those information (the confidential information shall be stored in a secure microcontroller for AP14 or higher).
Reasons		When communication between the microcontrollers of the in-vehicle part and the microcontroller and an external memory needs to contain CSPs ^{Δ4} for design

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		66/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

	reasons, they need to be designed so that they cannot be analyzed.
--	--

ID		VULCMN_02800 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs that communicate between microcontroller on in-vehicle parts / communicate between the microcontroller and external memory ^{Δ7}
	Target AP ^{Δ7}	20 ^{Δ4Δ5Δ7}
Requirements		By encrypting the communication between a microcontroller and a security chip on the in-vehicle part, analysis of confidential information shall be prevented.
Reasons		When confidential information needs to be transferred between the microcontroller and a security chip for design reasons, they need to be designed so that the confidential information cannot be analyzed.

4.4.2.2. Evaluation Requirements

ID		VULCMN_51800 ^{Δ6}
Application conditions ^{Δ12}	Functions/Parts	ECUs that communicate between microcontroller on in-vehicle parts / communicate between the microcontroller and external memory ^{Δ7}
	Target AP ^{Δ7}	All ^{Δ7}
Requirements		This requirement should be implemented when applying VULCMN_02700. The countermeasure requirements shall be satisfied through design verification.
Items to be checked		Whether countermeasures are implemented Validity of the countermeasures

ID		VULCMN_51900 ^{Δ6}
Application conditions ^{Δ12}	Functions/Parts	ECUs that communicate between microcontroller on in-vehicle parts / communicate between the microcontroller and external memory ^{Δ7}
	Target AP ^{Δ7}	20 ^{Δ7}
Requirements		This requirement should be implemented when applying VULCMN_02800. The countermeasure requirements shall be satisfied through design verification.
Items to be checked		Whether countermeasures are implemented Validity of the countermeasures

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		67/70
Application: In-vehicle parts in which information security countermeasures are implemented	No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a	

4.4.3. Tamper Resistance

4.4.3.1. Countermeasure Requirements

Physical analyses and attacks shall be prevented.

ID		VULCMN_02900 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs that require Authentication from a data center ^{Δ7Δ16}
	Target AP ^{Δ7}	20 ^{Δ4Δ5Δ7}
Requirements		CSP used for Authentication from a data center ^{Δ16} (*) ^{Δ8} shall be resistant to analysis by electromagnetic waves. (*) Key information (common key, private key) for client authentication, etc. ^{Δ8}
Reasons		To prevent CSPs ^{Δ4} in the chip from being analyzed through a side-channel attack.

ID		VULCMN_03000 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs that require Authentication from a data center ^{Δ7Δ16}
	Target AP ^{Δ7}	20 ^{Δ4Δ5Δ7}
Requirements		CSP used for Authentication from a data center ^{Δ16} (*) ^{Δ8} shall be resistant to analysis to measure current. (*) Key information (common key, private key) for client authentication, etc. ^{Δ8}
Reasons		To prevent CSPs ^{Δ4} in the chip from being analyzed through a side-channel attack.

ID		VULCMN_03100 ^{Δ6Δ12}
Application conditions ^{Δ6Δ12}	Functions/Parts	
	Target AP ^{Δ7}	
Requirements		(Deleted)
Reasons		

ID		VULCMN_03200 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs that require Authentication from a data center ^{Δ7Δ16}
	Target AP ^{Δ7}	20 ^{Δ4Δ5Δ7}
Requirements		To provide a voltage sensor.
Reasons		To prevent CPSs ^{Δ4} used for authentication from a data center ^{Δ16} in the chip from

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		68/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

	being analyzed through a side-channel attack, and to switch the security function upon receiving this detection signal to prevent further analysis or to help stop safely.
--	--

ID		VULCMN_03300 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs that require Authentication from a data center ^{Δ7Δ16}
	Target AP ^{Δ7}	20 ^{Δ4Δ5Δ7}
Requirements		To provide a frequency sensor.
Reasons		To prevent CSPs ^{Δ4} used for authentication from a data center ^{Δ16} in the chip from being analyzed through a side-channel attack, and to switch the security function upon receiving this detection signal to prevent further analysis or to help stop safely.

ID		VULCMN_03400 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	When VULCMN_00500 adopts access control to privileged functions or When VULCMN_02500 adopts access control to privileged functions ^{Δ7}
	Target AP ^{Δ7}	20 ^{Δ7}
Requirements		It is necessary to take measures (*) against authentication avoidance for access control to privileged functions and power glitch ^{Δ7} attacks that lead to false authentication. *) An example is to perform authentication judgment for access control to privileged functions multiple times. ^{Δ8}
Reasons		To prevent unauthorized rewriting of software from privileged functions ^{Δ7} due to authentication avoidance and authentication misjudgment.

ID		VULCMN_03500 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	ECUs that require Authentication from a data center ^{Δ7Δ16}
	Target AP ^{Δ7}	20 ^{Δ7}
Requirements		CSP used for authentication from a data center ^{Δ16} (*1) ^{Δ8} shall be resistant to timing analysis (*2). *1) Key information (common key, private key) for client authentication, etc. ^{Δ8} *2) For example, there are time smoothing and randomization of operations that handle CSP. ^{Δ8}
Reasons		To prevent CSPs in the chip from being analyzed through a side-channel attack.

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		69/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

4.4.3.2. Evaluation Requirements

ID		VULCMN_52000 ^{Δ6}
Application conditions ^{Δ12}	Functions/Parts	VULCMN_02900, VULCMN_03000, VULCMN_03400, VULCMN_03500. When even one of the above requirements is applied. ^{Δ7}
	Target AP ^{Δ7}	According to the target AP of the corresponding countermeasure requirements. ^{Δ7}
Requirements		The countermeasure requirements shall be satisfied through design verification.
Items to be checked		Whether countermeasures are implemented Validity of the countermeasures

ID		VULCMN_52100 ^{Δ6Δ12}
Application conditions ^{Δ12}	Functions/Parts	
	Target AP ^{Δ7}	
Requirements		(Deleted)
Items to be checked		

ID		VULCMN_52200 ^{Δ6}
Application conditions ^{Δ6Δ12}	Functions/Parts	VULCMN_03200, VULCMN_03300. When either is applied. ^{Δ7}
	Target AP ^{Δ7}	According to the target AP of the corresponding countermeasure requirements. ^{Δ7}
Requirements		The countermeasure requirements shall be satisfied through functional tests.
Items to be checked		Whether countermeasures are implemented Validity of countermeasures

In-Vehicle Network	Requirements Specification of Common Vulnerability Countermeasure		70/70
Application: In-vehicle parts in which information security countermeasures are implemented		No.	SEC-ePF-VUL-CMN-REQ-SPEC-a01-09-a

5. Deleted ^{Δ6 Δ14}

5.1. Deleted ^{Δ6 Δ14}

ID		VULCMN_52300
Application conditions ^{Δ12}	Functions/Parts	-
	Target AP ^{Δ7}	-
Requirements		Deleted.
Reasons		-
Reference requirements		-