オートモーティブソフトウェアの脆弱性とソフトウェア開発ライフサイクルにおけるセキュリティソリューション

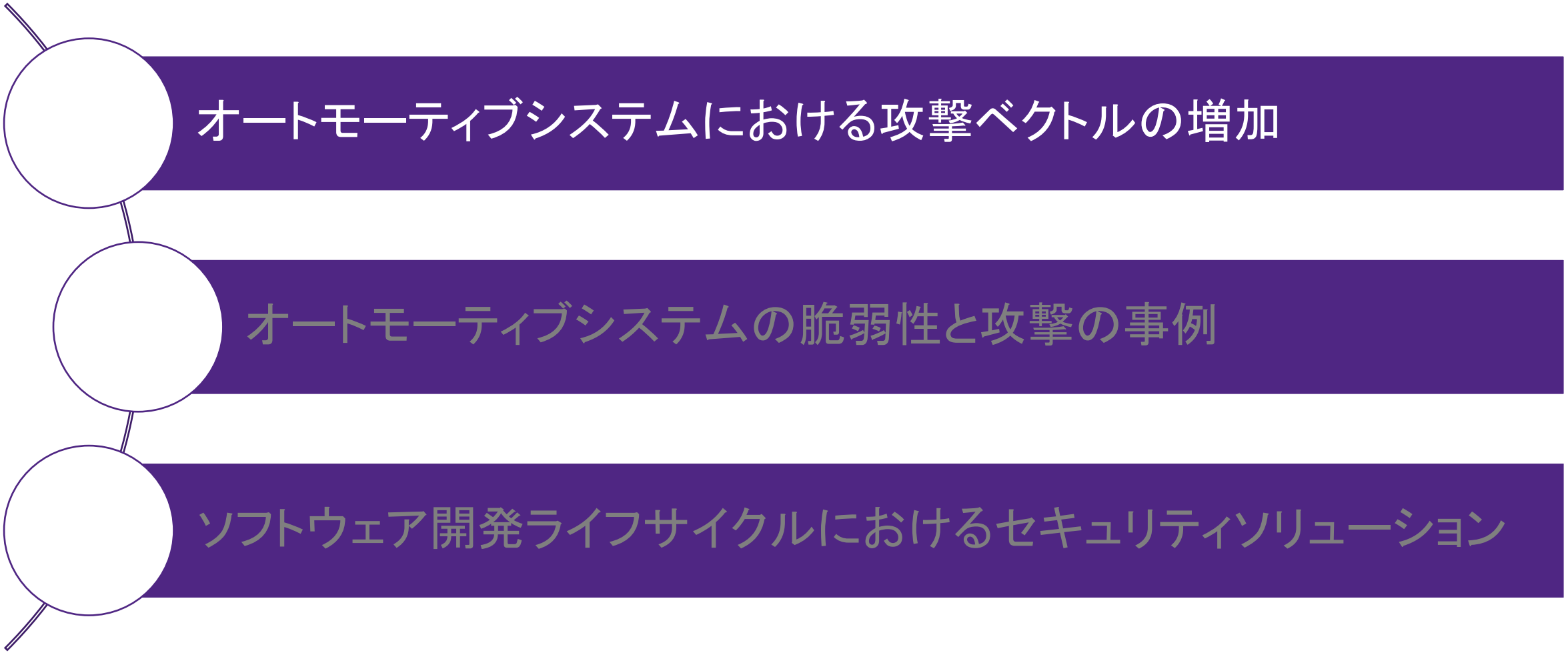
プリンシパルオートモーティブセキュリティストラテジスト
岡　デニス　健五
dennis.kengo.oka@synopsys.com

車載組込みシステムフォーラム (ASIF) 2020年度第4回
2021/2/22

アジェンダ

- オートモーティブシステムにおける攻撃ベクトルの増加
- オートモーティブシステムの脆弱性と攻撃の事例
- ソフトウェア開発ライフサイクルにおけるセキュリティソリューション

アジェンダ



IVI: In-Vehicle Infotainment
OSS: Open Source Software
V2X: Vehicle-to-Everything

自動車業界の動向

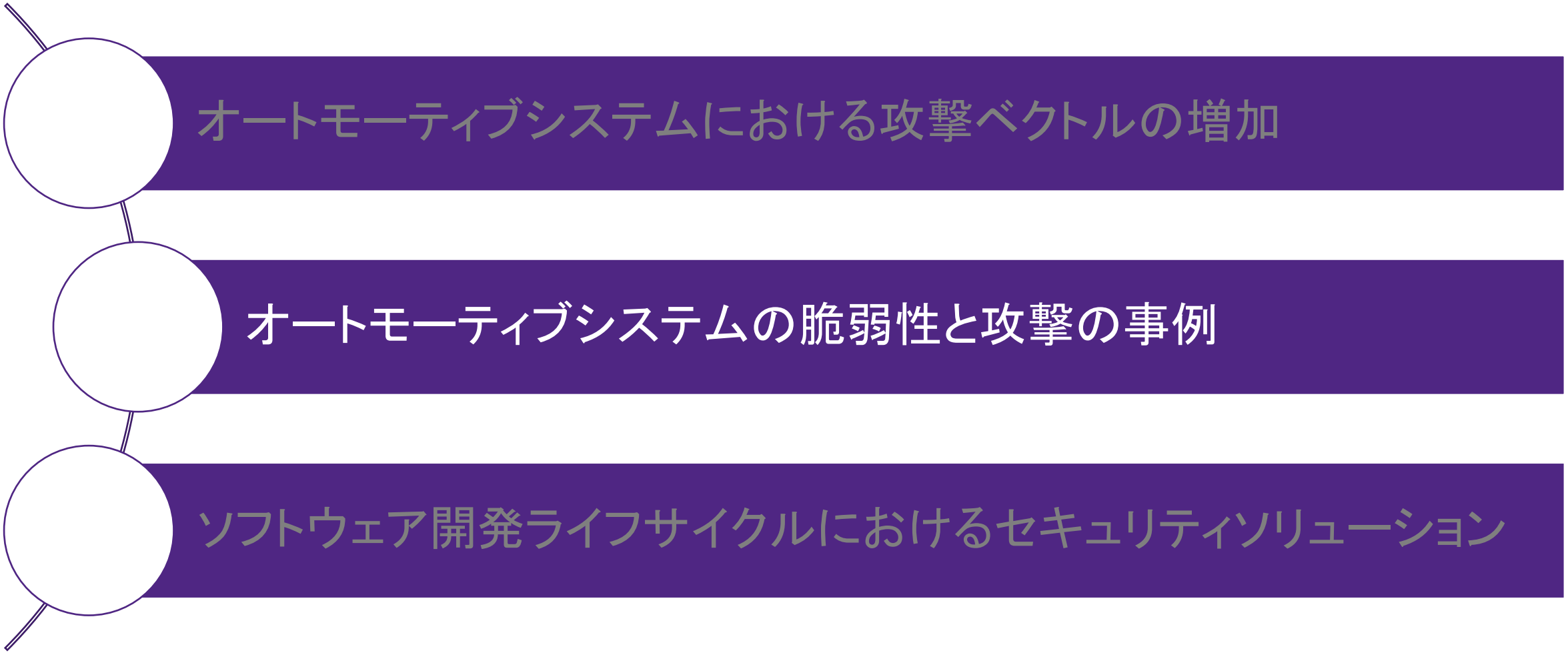
- CASE
  - コネクテッド
  - 自動運転
  - シェアリングとサービス
  - 電動化
- ソフトウェアの増加
  - 1億行以上
  - オープンソースソフトウェア (OSS)
- 複数の無線インターフェース
  - Bluetooth
  - Wi-Fi
  - Cellular
  - GPS
  - V2X

IVI: In-Vehicle Infotainment
V2X: Vehicle-to-Everything
JTAG: Joint Test Action Group

攻撃ベクトル

Wi-Fi
Bluetooth
Cellular
USB
SD
GPS
ECU
Firmware/Software
IVI
Software
CAN
(OBD-2)
V2X
Automotive
Ethernet
JTAG
Camera
Sensor

アジェンダ



2つの事例

攻撃の事例 #1

- Bluetooth通信　(Wi-Fi)
- 複数のステップを実施
- ファームウェアアップデート
- 任意のコントロール
- リモートからCAN通信
- 対象ECUへの不正な故障診断メッセージ

攻撃の事例 #2

- Bluetooth通信
- 複数のステップを実施
- ファームウェアアップデート
- 任意のコントロール
- 物理的アクセスによるCAN通信
- 車両の盗難

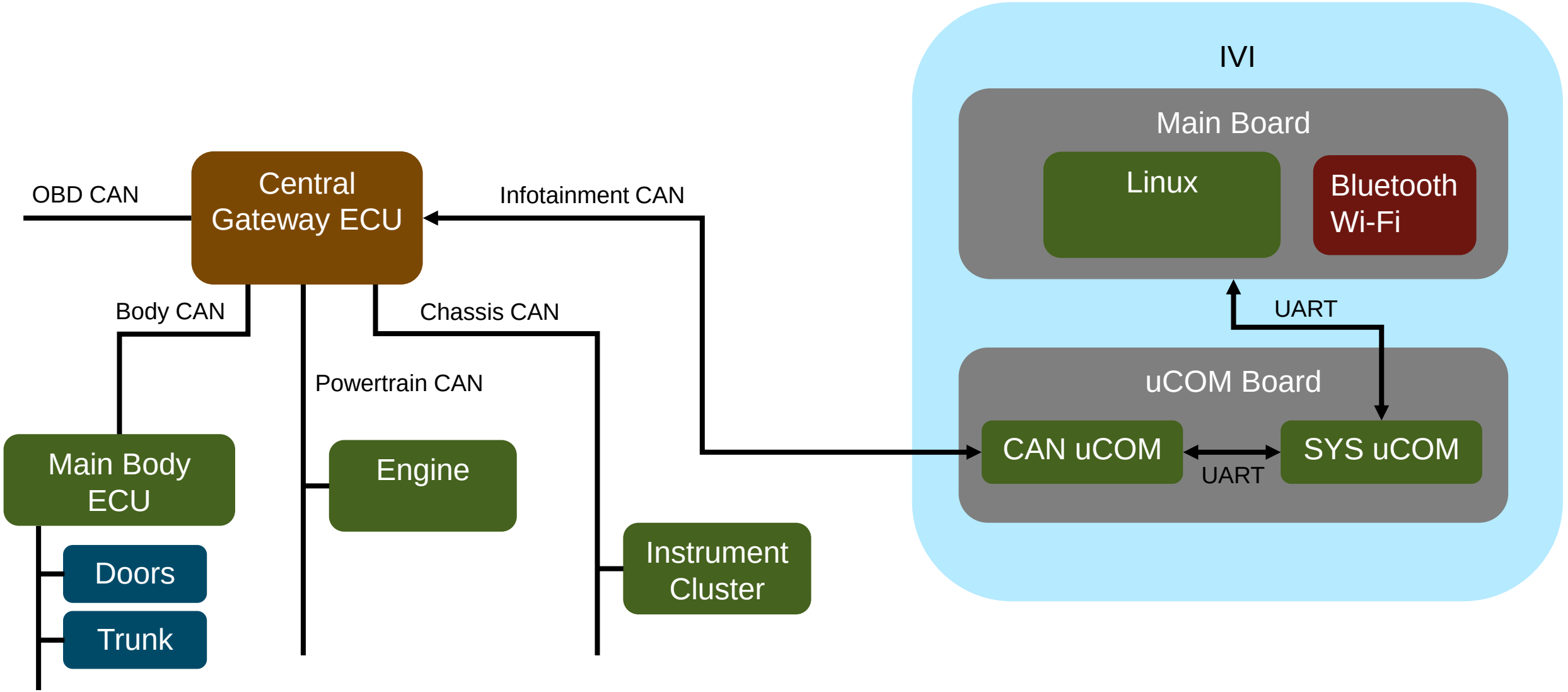
Ref: Designed by Freepik

Ref: https://keenlab.tencent.com/en/2020/03/30/Tencent-Keen-Security-Lab-Experimental-Security-Assessment-on-Lexus-Cars/
https://www.esat.kuleuven.be/cosic/news/belgian-security-researchers-from-cosic-and-imec-steal-a-tesla-model-x-in-minutes/

攻撃の事例 #1

IVI: In-Vehicle Infotainment
UART: Universal Asynchronous Receiver/Transmitter
OBD: On-Board Diagnostics

システムの概要

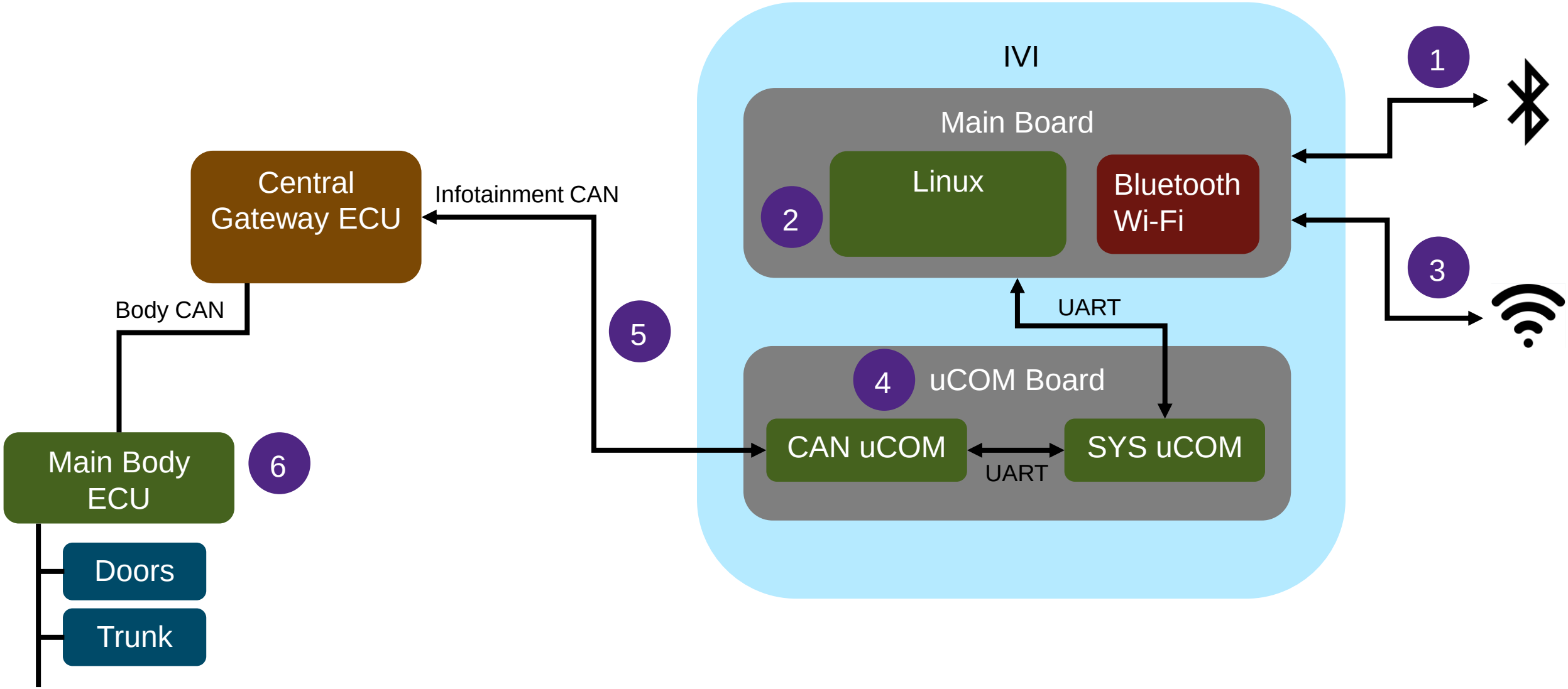


脆弱性と弱点のまとめ

#	コンポーネント	脆弱性・弱点	結果
1	Main Board	Bluetoothペアリング前の接続機能の実装の脆弱性	Bluetoothの脆弱性を悪用することによる任意のコード実行
2	Main Board	セキュアブートなし	カスタムブート、システムの改ざん
3	uCOM Board	ファームウェアアップデートのデジタル署名認証なし	UARTを介した悪意のあるファームウェアアップデート（セキュリティ対策が実施されていない）
4	Main Body ECU	故障診断メッセージに対する認証なし	CANを介した不正な故障診断メッセージがMain Body ECUで実行

IVI: In-Vehicle Infotainment
UART: Universal Asynchronous Receiver/Transmitter

攻撃パス



「責任ある開示」（Responsible Disclosure）

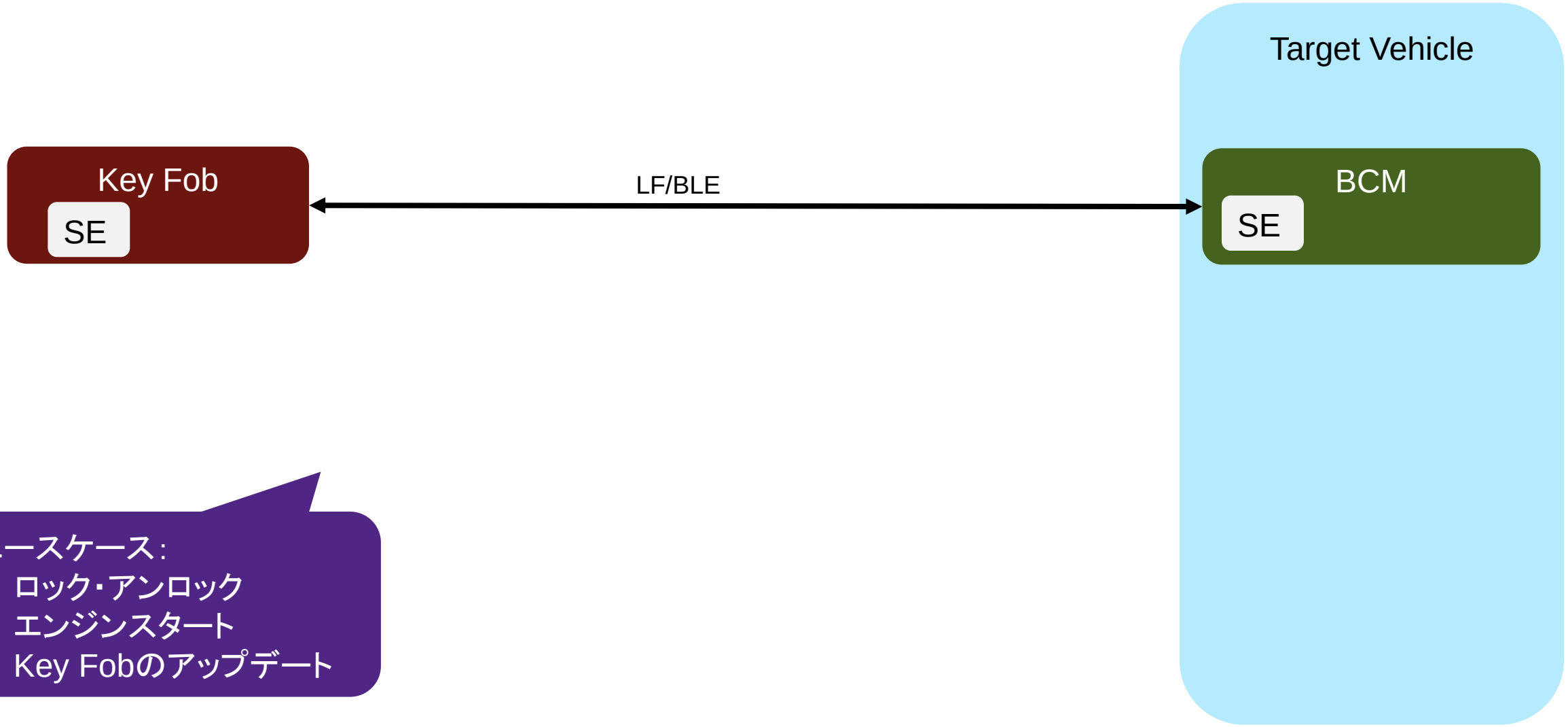
- 2019年10月セキュリティリサーチャーがOEMに対し報告
  - 「責任ある開示」（Responsible Disclosure）
- 2019年12月OEMが課題を確認
- 2020年3月OEMが技術的な対策を公開
- 2020年3月セキュリティリサーチャーが課題のサマリーを公開

Ref: Designed by Freepik

攻撃の事例 #2

SE: Secure Element
BCM: Body Control Module
LF: Low Frequency
BLE: Bluetooth Low Energy

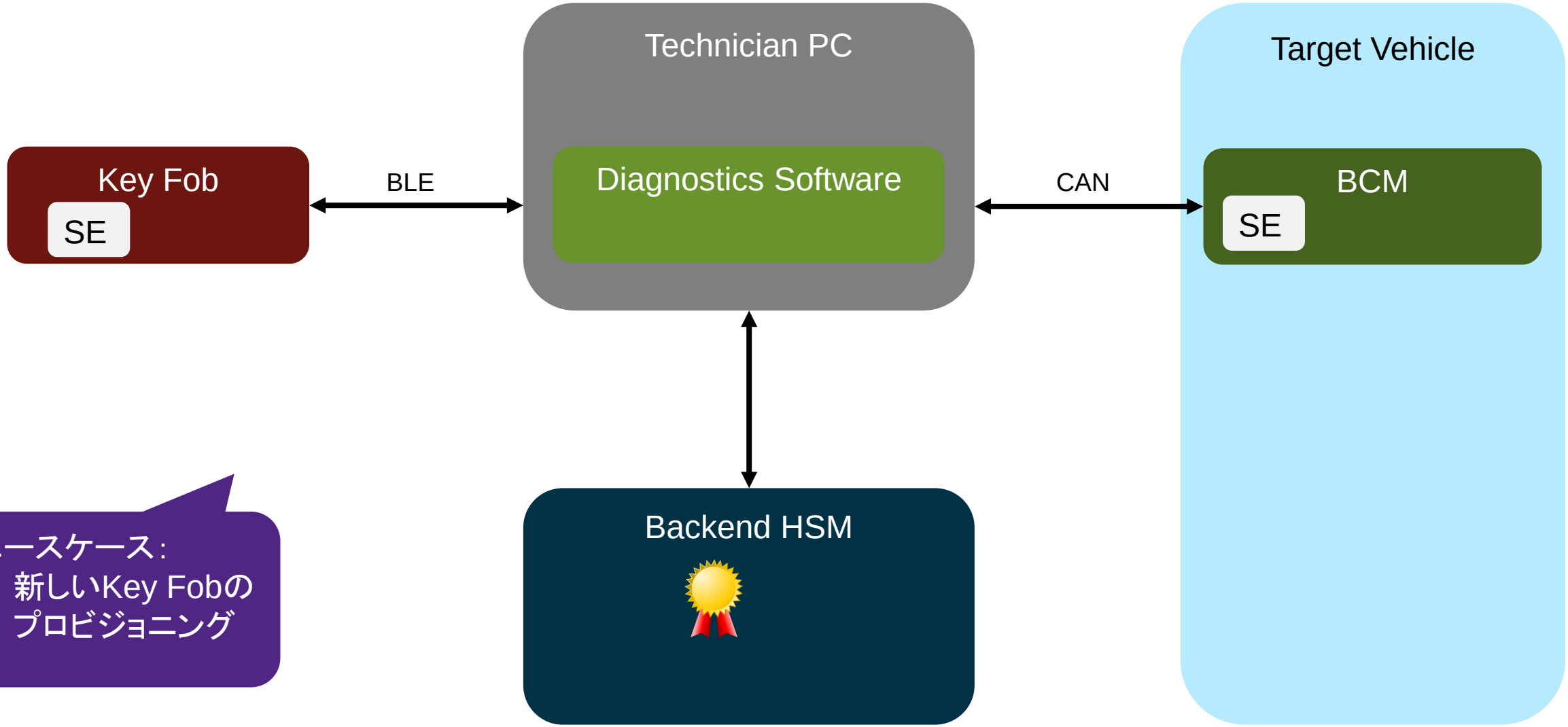
システムの概要 (1)



ユースケース:
- ロック・アンロック
- エンジンスタート
- Key Fobのアップデート

システムの概要 (2)

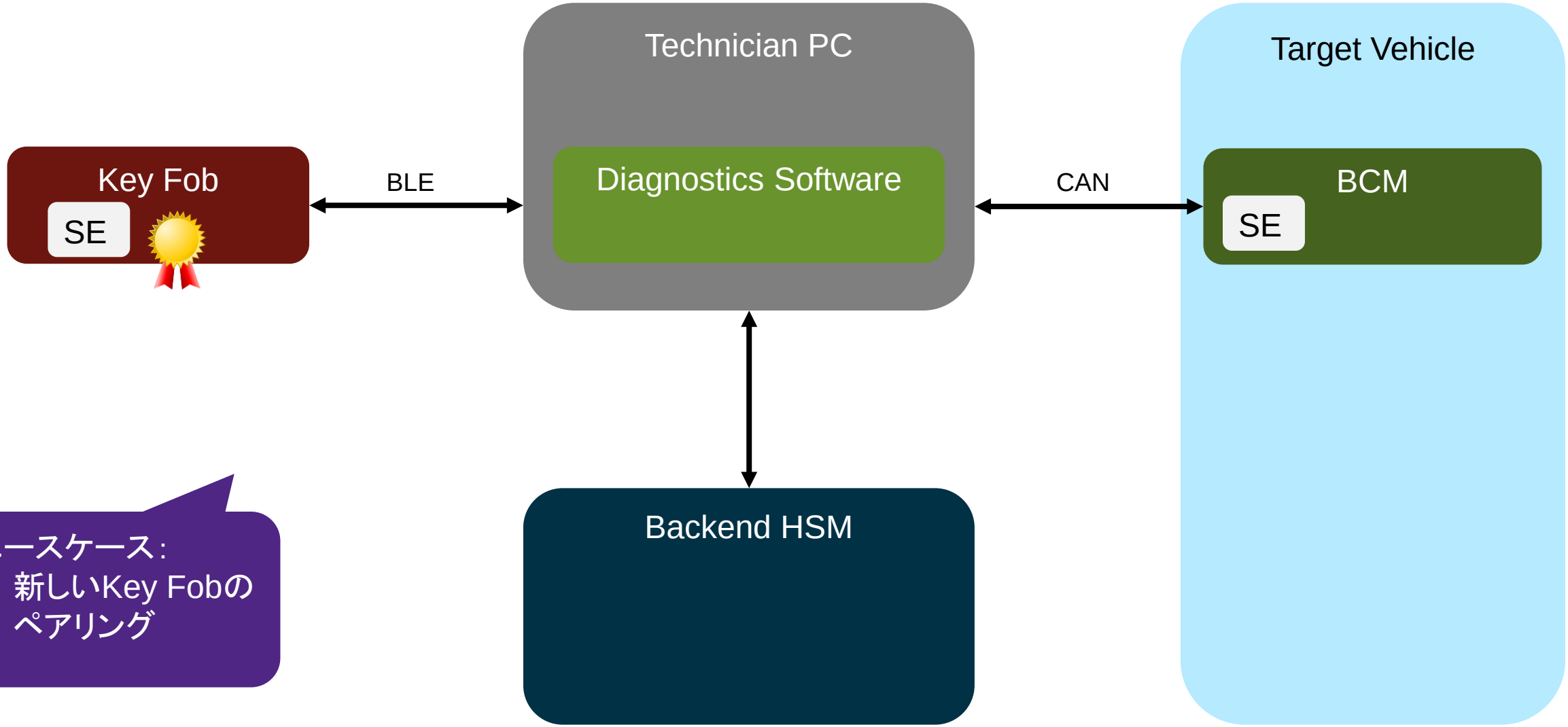
SE: Secure Element
BCM: Body Control Module
LF: Low Frequency
BLE: Bluetooth Low Energy
HSM: Hardware Security Module



ユースケース:
- 新しいKey Fobのプロビジョニング

システムの概要 (3)

SE: Secure Element
BCM: Body Control Module
LF: Low Frequency
BLE: Bluetooth Low Energy
HSM: Hardware Security Module



ユースケース:
- 新しいKey Fobのペアリング

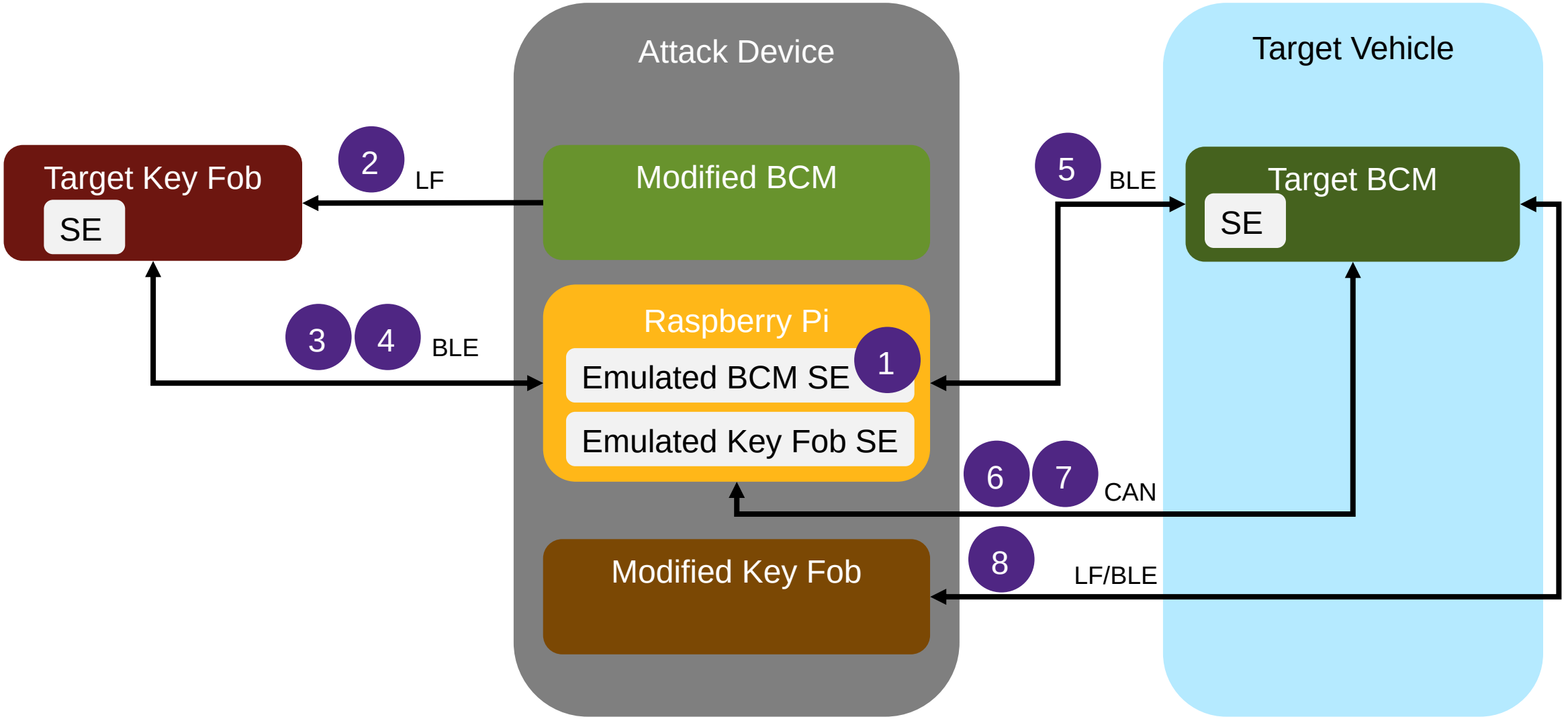
BCM: Body Control Module
BLE: Bluetooth Low Energy

脆弱性と弱点のまとめ

#	コンポーネント	脆弱性・弱点	結果
1	Key Fob	ファームウェアアップデート機能の署名検証の実装の脆弱性	BLEを介してターゲットKey Fobに悪意のあるファームウェアアップデート
2	BCM	Key Fobの証明書の検証なし	ターゲット車両のBCMと攻撃者のKey Fobのペアリング

SE: Secure Element
BCM: Body Control Module
LF: Low Frequency
BLE: Bluetooth Low Energy

攻撃パス

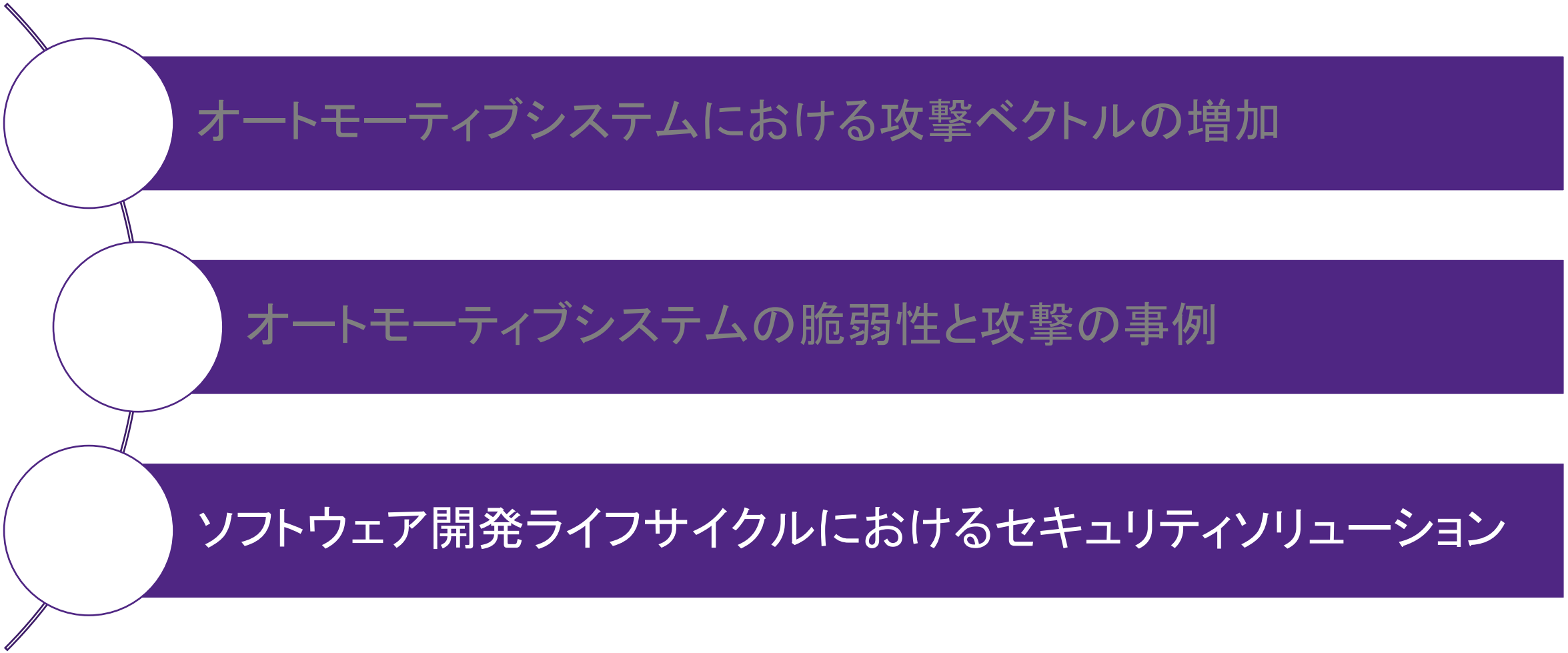


「責任ある開示」（Responsible Disclosure）

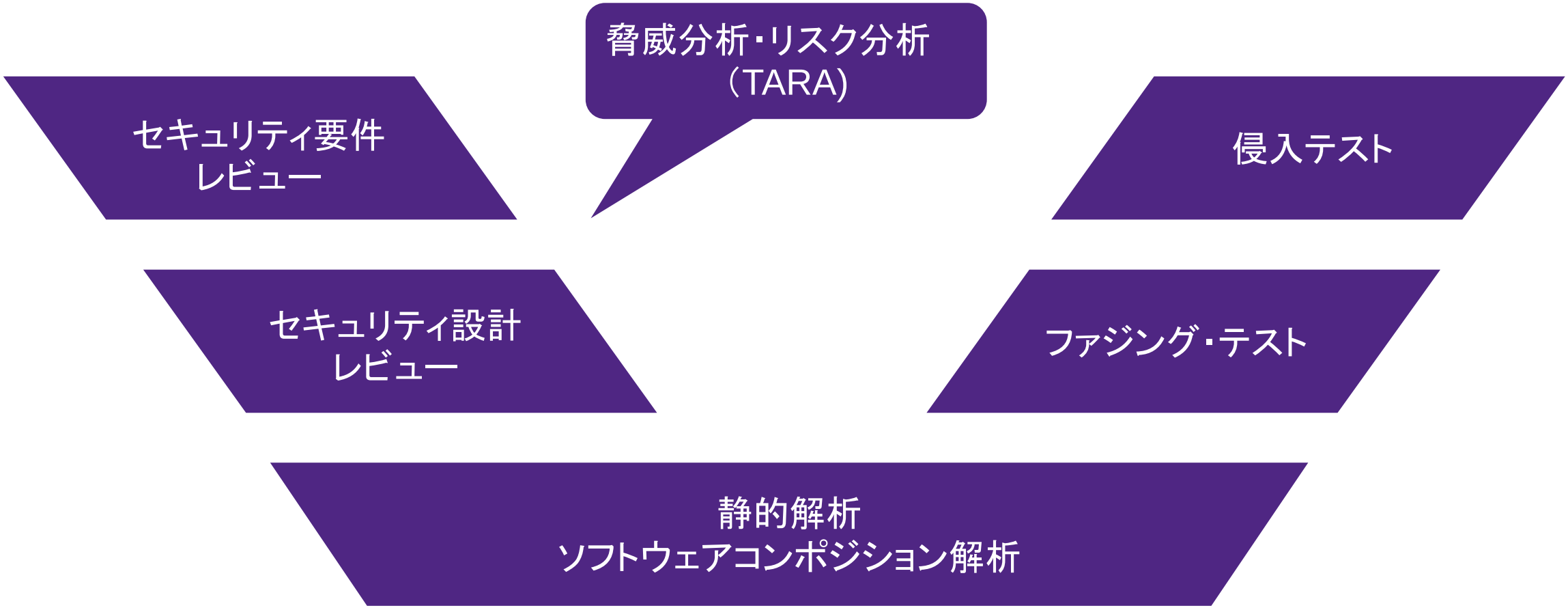
- 2020年8月セキュリティリサーチャーがOEMに対し報告
  - 「責任ある開示」（Responsible Disclosure）
- 2020年11月OEMがパッチをOTAでリリース
- 2020年11月セキュリティリサーチャーが課題のサマリーを公開

Ref: Designed by Freepik

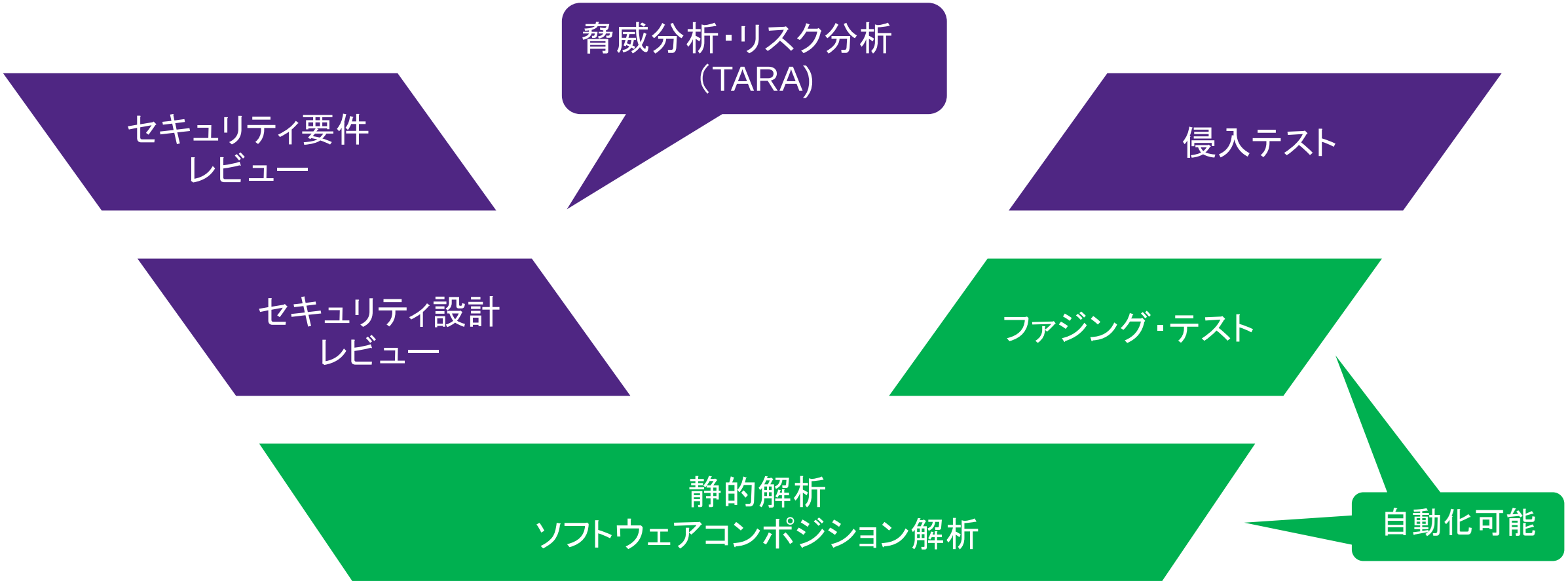
アジェンダ

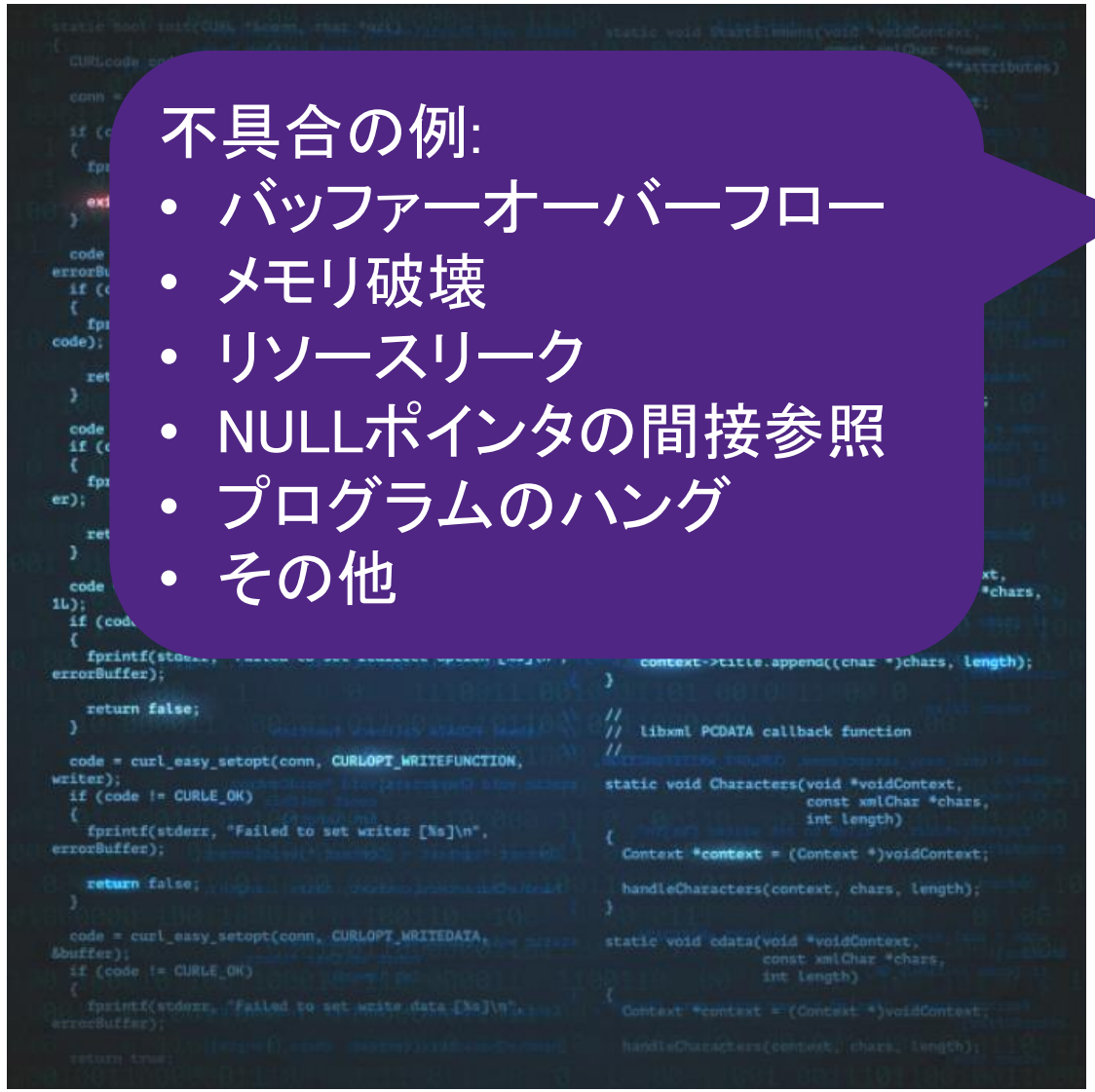


V字モデルにおけるセキュリティソリューション



V字モデルにおけるセキュリティソリューション





静的解析

- ソースコードを解析し不具合を発見する技術
- ソフトウェア自体を実行しない
- テストケース不要

コーディング規約チェックのサポート:
- CERT C/C++
- MISRA C/C++
- AUTOSAR C++

Ref: Designed by Freepik

SBOM: Software Bill Of Materials
OSS: Open Source Software

ソフトウェア・コンポジション解析

- オープンソースの管理
- セキュリティ/ライセンス/運用リスクを特定
- SBOMの生成

ソフトウェア

- オープンソース ソフトウェア (OSS)
- 自社開発の ソフトウェア
- 商用ソフトウェア
- アウトソース開発 によるソフトウェア

Ref: Designed by Freepik

ファジング・テスト

- 未知の脆弱性のテスト
- 不具合を検出するため
  意図的に不正入力
- 各種プロトコルに対する
  不正な入力パターン

Ref: Designed by Freepik

攻撃の事例 #1

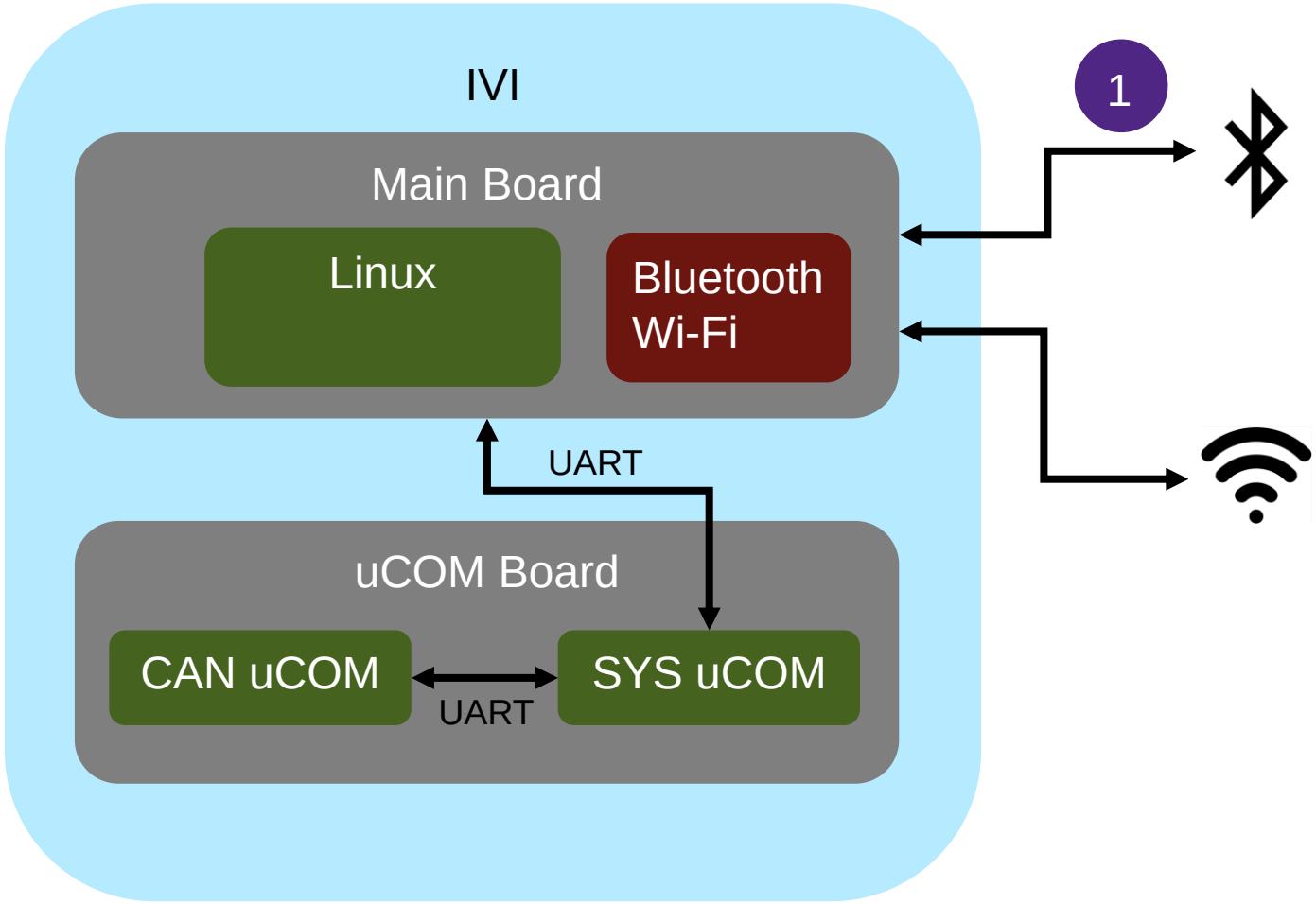
ソフトウェア開発ライフサイクルにおけるセキュリティソリューション

OSS: Open Source Software
IVI: In-Vehicle Infotainment
UART: Universal Asynchronous Receiver/Transmitter

攻撃パス：1に対するセキュリティソリューション

- 静的解析
- ソフトウェアコンポジション解析
- ファジング・テスト
- 侵入テスト

- Bluetooth実装の脆弱性の発見
- Bluetoothの脆弱なOSSコンポーネントの管理
- …

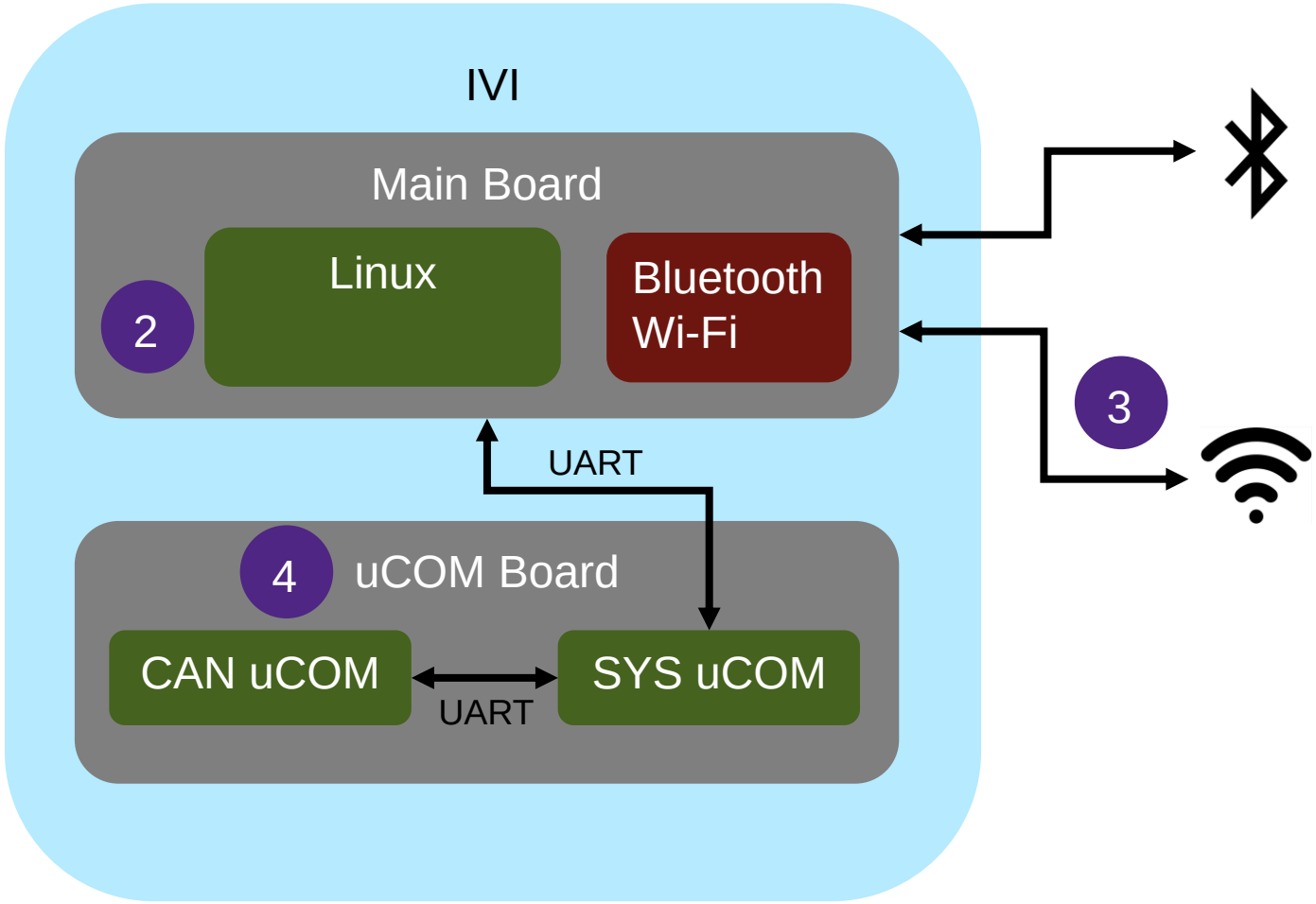


TARA: Threat Analysis and Risk Assessment
IVI: In-Vehicle Infotainment
UART: Universal Asynchronous Receiver/Transmitter

攻撃パス：2、3、4に対するセキュリティソリューション

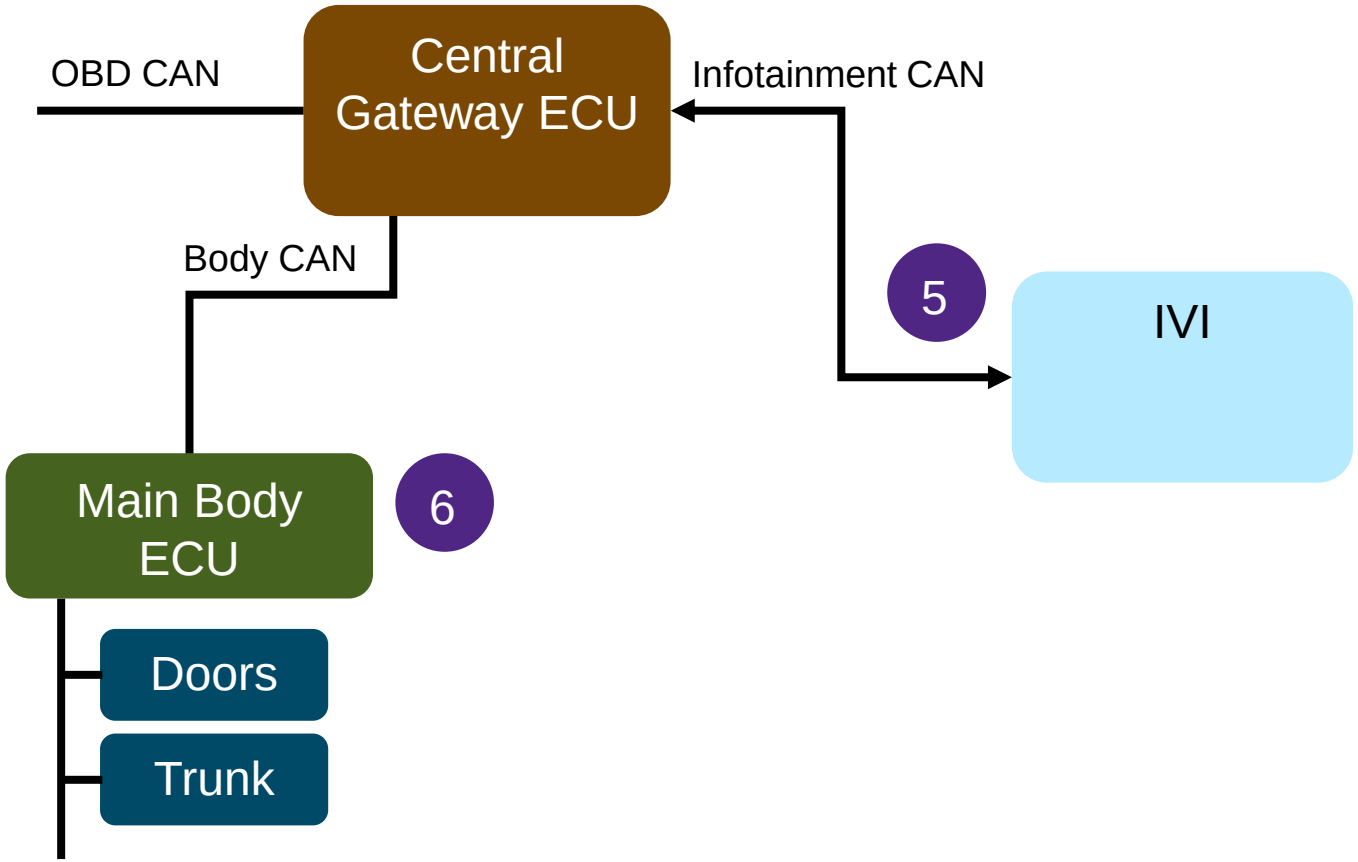
- セキュリティ要件レビュー
- セキュリティ設計レビュー
- 脅威分析・リスク分析 (TARA)
- 侵入テスト

- セキュアブート欠如の発見
- ファームウェアアップデートに関するデジタル署名認証欠如の発見
- …



IVI: In-Vehicle Infotainment
TARA: Threat Analysis and Risk Assessment
SecOC: Secure Onboard Communication

攻撃パス：5，6に対するセキュリティソリューション



- セキュリティ要件レビュー
- セキュリティ設計レビュー
- 脅威分析・リスク分析 (TARA)
- ファジング・テスト
- 侵入テスト

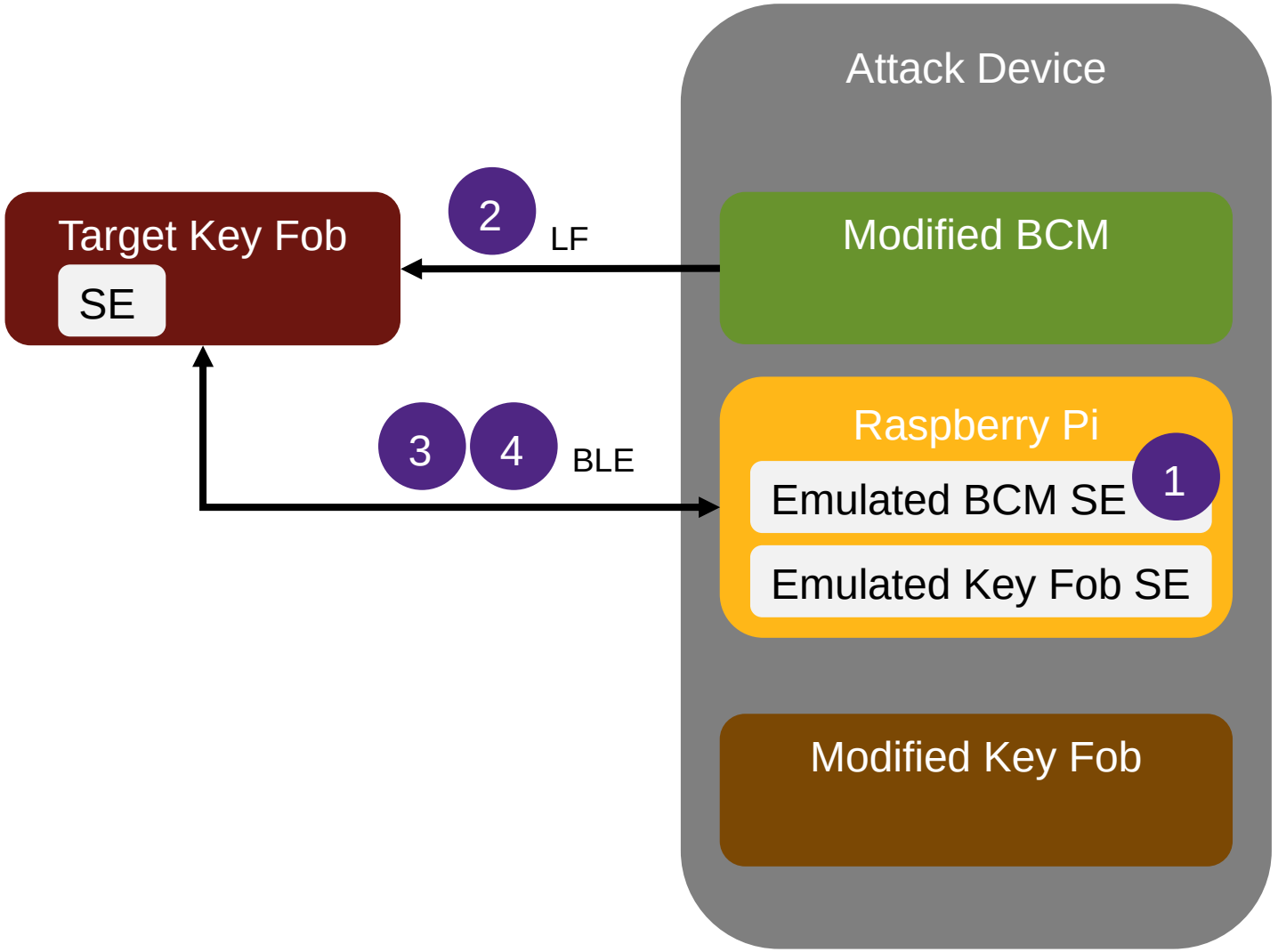
- 故障診断メッセージの認証欠如の発見
- Central Gateway ECUのセキュアルーティング欠如の発見
- CANバスのSecOC欠如の発見
- …

攻撃の事例 #2

ソフトウェア開発ライフサイクルにおけるセキュリティソリューション

SE: Secure Element
BCM: Body Control Module
LF: Low Frequency
BLE: Bluetooth Low Energy
OSS: Open Source Software

攻撃パス：3，4に対するセキュリティソリューション



- 静的解析
- ソフトウェアコンポジション解析
- ファジング・テスト
- 侵入テスト

- ファームウェアアップデートの署名検証の実装の脆弱性の発見
- Bluetoothの脆弱なOSSコンポーネントの管理
- …

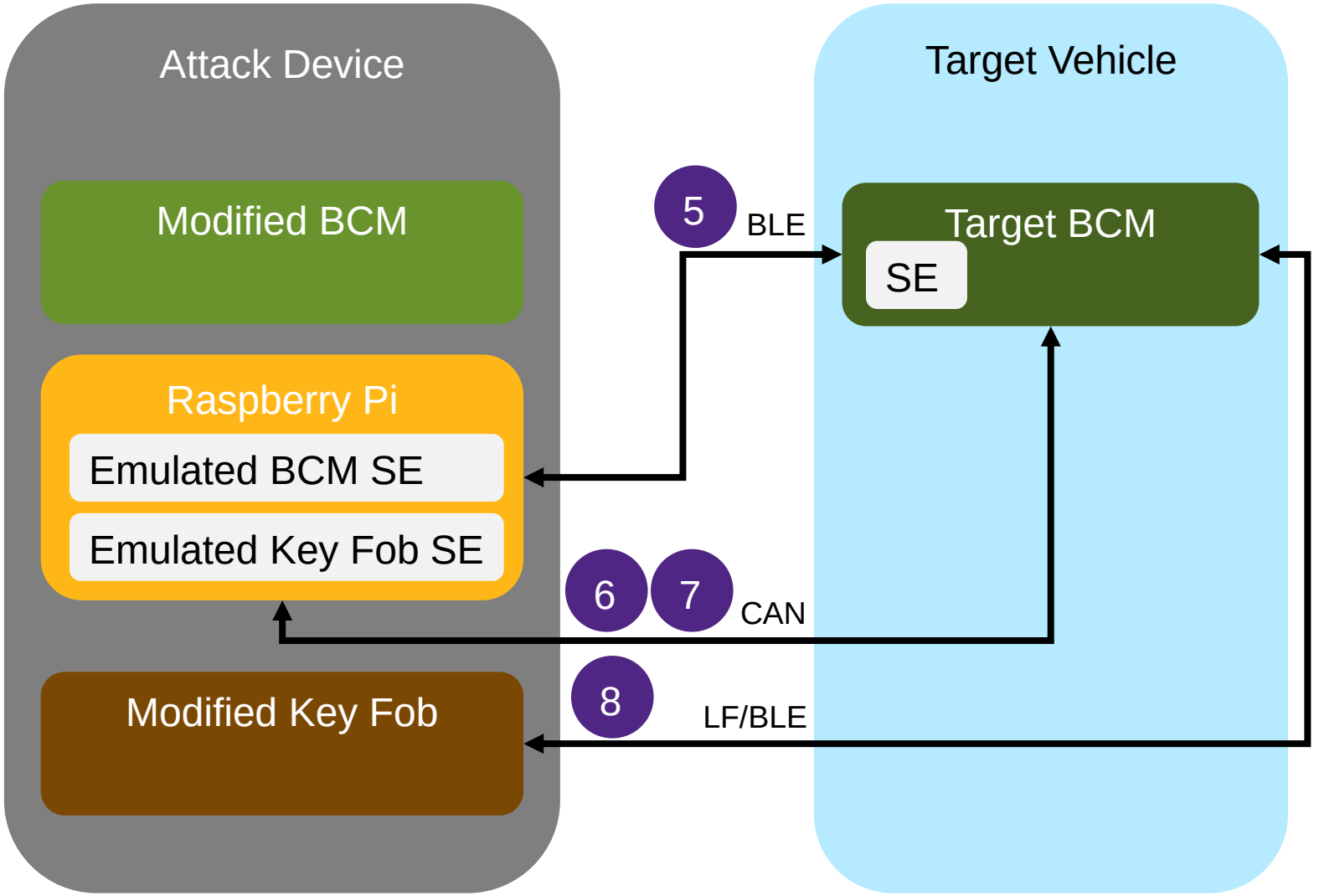
SE: Secure Element
BCM: Body Control Module
LF: Low Frequency

BLE: Bluetooth Low Energy
TARA: Threat Analysis and Risk Assessment

攻撃パス：6，7に対するセキュリティソリューション

- セキュリティ要件レビュー
- セキュリティ設計レビュー
- 脅威分析・リスク分析 (TARA)
- 侵入テスト

- Key Fobの証明書の検証欠如の発見
- 故障診断アクセスに関する認証欠如の発見
- …



dennis.kengo.oka@synopsys.com

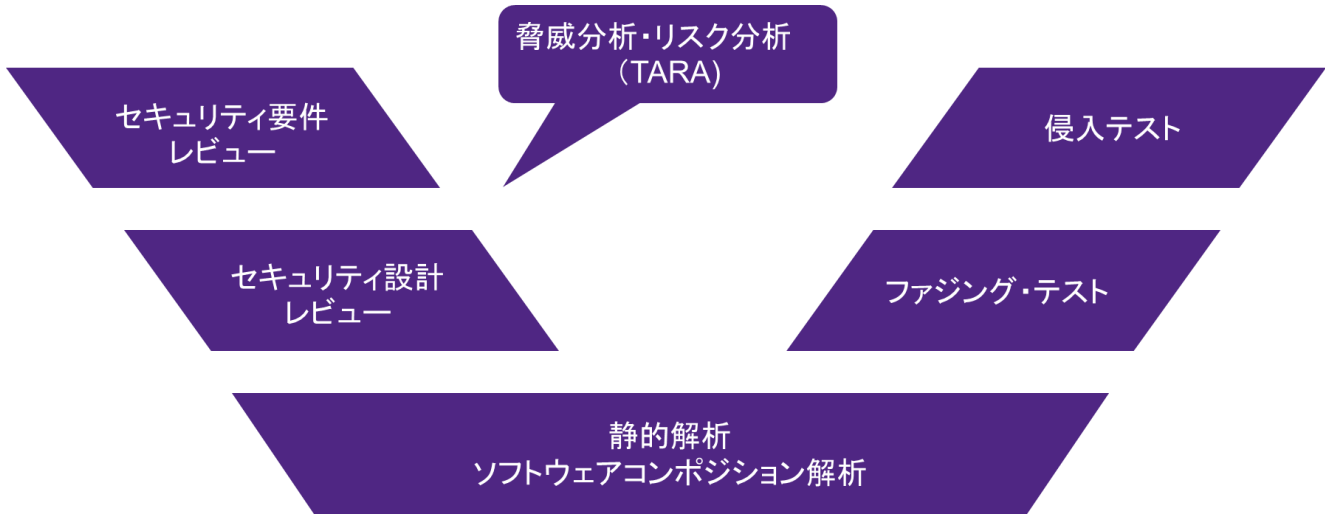
重要なポイント：Call to Action

オートモーティブシステムの攻撃ベクトルを把握する

- 通信インターフェース
- より多くのソフトウェア (例えば、OSS)

ソフトウェア開発ライフサイクルに適切なセキュリティソリューションを適用

- セキュリティ要件レビュー
- セキュリティ設計レビュー
- 脅威分析・リスク分析（TARA)
- 静的解析
- ソフトウェア・コンポジション解析
- ファジング・テスト
- 侵入テスト



SYNOPSYS®
Silicon to Software™

Thank You