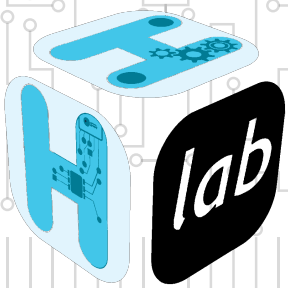
H2LAB-STIG-PHY
05-2026

Systèmes embarqués : guide des mécanismes de protection physique



STIG H²Lab

Informations

Créée en 2020, H2Lab est une association loi 1901 dont l'objectif est de concevoir, développer et diffuser des solutions open-hardware et open-source dédiées à l'expérimentation autour des systèmes embarqués.
Ses principaux axes de travail sont :

- Conception de plateformes matérielles pour l'analyse hardware et software
- Développement d'alternatives ouvertes aux outils propriétaires, souvent opaques
- Publication de guides techniques et de recommandations pour promouvoir les bonnespratiques en matière de sécurité, de confidentialité et de durabilité dans l'écosystèmedes objets connectés et des systèmes embarqués

Soutien aux chercheurs, enseignants et étudiants via la mise à disposition d'outils, de contenus pédagogiques et de formations.
Partenariats académiques pour encourager la mutualisation des ressources et des savoirs.

Historique des révisions

Version	**Date**	**Auteur**	**Modifications**
1.0	Mai 2026	H2Lab	Version initiale du guide
1.1	Août 2026	H2Lab	Reprise de forme, ajout de la licence

Table des matières

Glossaire des acronymes

0.1 Glossaire

Attaque par canal auxiliaire
: Technique d'extraction d'information exploitant des mesures physiques indirectes (consommation, rayonnement électromagnétique, temps d'exécution) sans altérer le fonctionnement du composant.

Attaque par faute
: Technique consistant à perturber volontairement l'alimentation, l'horloge ou l'environnement d'un composant pour provoquer un comportement anormal exploitable.

Attaque semi-invasive
: Classe d'attaques nécessitant une ouverture partielle du boîtier (décapsulation) sans altération électrique directe du circuit, par opposition aux attaques invasives.

BootROM
: Mémoire morte interne au SoC exécutée en tout premier lors du démarrage, généralement non modifiable après fabrication.

Chaîne de confiance
: Ensemble ordonné des étapes de vérification cryptographique reliant la racine de confiance au logiciel applicatif final.

Défense en profondeur
: Principe de sécurité consistant à superposer plusieurs mécanismes de protection indépendants afin qu'une défaillance isolée ne compromette pas l'ensemble du système.

Élément sécurisé
: Composant matériel dédié au stockage et à la manipulation de secrets cryptographiques, conçu pour résister aux attaques physiques et logiques.

Enfouissement de pistes
: Technique de routage PCB consistant à placer les pistes sensibles sur des couches internes afin de limiter leur accessibilité physique.

Micro-sondage (probing)
: Technique d'attaque consistant à contacter directement une piste ou un point de test avec une sonde fine pour observer ou injecter un signal.

Mode DFU / mode usine
: Mode de fonctionnement privilégié destiné à la mise à jour ou à la production, offrant des capacités étendues devant être strictement contrôlées en exploitation.

Politique anti-retour arrière (anti-rollback)
: Mécanisme empêchant l'installation d'une version de firmware antérieure à une version minimale autorisée, afin d'empêcher la réintroduction de vulnérabilités corrigées.

Racine de confiance
: Ensemble minimal de code et de clés cryptographiques, résistant à la modification, à partir duquel repose l'intégralité de la chaîne de vérification du démarrage.

Reballing
: Opération de reconstruction des billes de soudure d'un boîtier BGA, utilisée notamment lors d'un rework ou d'une attaque nécessitant la dépose du composant.

Rework
: Ensemble des opérations de dépose, modification et repose de composants sur un PCB, pouvant être détourné à des fins offensives (interposition, substitution).

Secure Boot
: Mécanisme de démarrage sécurisé vérifiant l'authenticité et l'intégrité de chaque étape logicielle avant son exécution.

TEE (environnement d'exécution de confiance)
: Zone d'exécution isolée du système d'exploitation principal, garantissant la confidentialité et l'intégrité du code et des données qui y sont traités.

Vias bouchés/masqués
: Techniques de fabrication PCB rendant les vias de transition inaccessibles en surface, limitant les points d'accroche pour une micro-sonde.

0.2 Liste des acronymes

AHB Advanced High-performance Bus.

APB Advanced Peripheral Bus.

API Application Programming Interface.

AVA_VAN Classe Common Criteria d'évaluation du potentiel d'attaque.

BIOS Basic Input/Output System.

BGA Ball Grid Array.

CC Common Criteria.

CERT Computer Emergency Response Team.

CISA Cybersecurity and Infrastructure Security Agency.

CPU Central Processing Unit.

CVE Common Vulnerabilities and Exposures.

CWE Common Weakness Enumeration.

DFU Device Firmware Update.

DSP Digital Signal Processor.

EEPROM Electrically Erasable Programmable Read-Only Memory.

FPGA Field-Programmable Gate Array.

FSBL First Stage Boot Loader.

GPIO General Purpose Input/Output.

I2C Inter-Integrated Circuit.

ICS Industrial Control Systems.

IP Intellectual Property (bloc matériel intégré).

ISMS Information Security Management System.

HSE Hardware Security Engine.

JTAG Joint Test Action Group (IEEE 1149.x).

MAC Media Access Control.

MITM Man-In-The-Middle.

MCO/MCS Maintien en condition opérationnelle / sécurité.

MMU Memory Management Unit.

NIST National Institute of Standards and Technology.

NOR/NAND Technologies de mémoire flash non volatile.

PCB Printed Circuit Board.

PHY Couche physique de communication.

RAM/SRAM Random Access Memory / Static RAM.

ROM Read-Only Memory.

RTOS Real-Time Operating System.

SoC System on Chip.

SPI Serial Peripheral Interface.

SSBL Second Stage Boot Loader.

TPM Trusted Platform Module.

TEE Trusted Execution Environment.

TrustZone Technologie ARM de cloisonnement sécurisé.

UART Universal Asynchronous Receiver-Transmitter.

USB Universal Serial Bus.

1
Introduction et périmètre

1.1 Objectif du guide

Ce guide formalise un ensemble d'exigences techniques applicables à la conception et à l'évaluation de la cybersécurité des systèmes embarqués. Le document couvre la chaîne matérielle et logicielle, depuis l'accès physique jusqu'aux mécanismes de démarrage sécurisé.

1.2 Périmètre technique

Le périmètre traite :

- les équipements embarqués à base de SoC, microcontrôleur ou FPGA ;
- les interfaces physiques et logiques accessibles en laboratoire ;
- les contre-mesures de protection physique (scellés, capteurs, effacement) ;
- les mécanismes logiciels de confiance (secure boot, TEE, MCO/MCS).

1.3 Niveaux de sécurité et menaces

Le guide utilise les niveaux d'attaquant standards des Critères Communs (famille AVA_VAN, Common Criteria Part 3 [10]) :

- **Basic** : capacités et moyens limités ;
- **Enhanced-Basic** : attaquant outillé avec effort accru ;
- **Moderate** : compétences confirmées et moyens de laboratoire ;
- **High** : attaquant expert, moyens avancés et temps long.

Dans ce guide, une exigence est associée à un niveau AVA_VAN minimal attendu.
Les menaces de référence sont :

- **T01** ouverture non autorisée du boîtier ;
- **T02** extraction ou remplacement de composants ;
- **T03** abus des interfaces de debug et de test ;

- **T04** compromission de la mise à jour ou du démarrage ;
- **T05** fuite d'information par bus ou mémoire externe.

1.4 Synthèse opérationnelle

1.4.1 Principes directeurs

- Concevoir l'équipement avec une vision cycle de vie complet (MCO/MCS).
- Verrouiller les interfaces de test dès la phase d'industrialisation.
- Appliquer la défense en profondeur : passif + actif + vérification logicielle.
- Mesurer et tracer : sans preuve de vérification, il n'y a pas de sécurité exploitable.

1.4.2 Priorisation des actions

1. Établir la cartographie matérielle/logicielle et la criticité des actifs.
2. Traiter en priorité les voies d'accès physique et debug non maîtrisées.
3. Durcir la chaîne de boot et la mise à jour avant extension fonctionnelle.
4. Mettre en place une vérification périodique des protections d'autoprotection.

1.5 Schéma 1 – Surface d'attaque physique

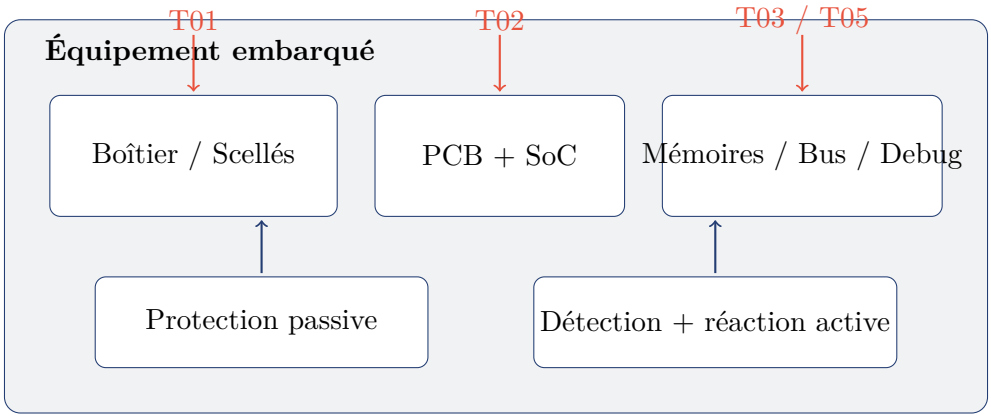


FIGURE 1.1 – Vue de synthèse de l'exposition physique et des contre-mesures.

2

Écosystème des systèmes embarqués

2.1 Diversité des cibles

L'écosystème couvre des objets grand public (clé USB, smartphone), industriels (automates, ferroviaire), transport (avionique) et contrôle d'accès. La conséquence directe est une forte variabilité des contraintes de puissance, de maintenance et de durée de vie.

2.2 Architecture de référence

Les plateformes modernes reposent majoritairement sur des SoC intégrant CPU, contrôleurs mémoire, accélérateurs et interfaces d'entrée/sortie. La connectivité externe est assurée via GPIO et contrôleurs dédiés, tandis que les bus internes (AHB/APB par exemple) restent invisibles hors puce.

REQ_ARCH_01 – Cartographie d'architecture

Le fabricant doit produire une cartographie maintenue du produit : SoC, mémoires volatiles et non volatiles, coprocesseurs, interfaces exposées, points de test et chemins de démarrage. La cartographie est versionnée à chaque évolution matérielle et logicielle.

- Niveau d'attaquant minimal : **AVA_VAN.Basic**.
- Menace ciblée : **T02** et **T03**.
- Sans inventaire technique fiable, les surfaces d'attaque réelles ne sont pas maîtrisées et les analyses ultérieures ne sont pas reproductibles.
- Références : NIST SP 800-193 (résilience firmware), BSI IT-Grundschutz Compendium (modélisation des menaces) [23, 8].

État de l'art des attaques. Les campagnes de reverse engineering matériel exploitent en priorité l'absence de cartographie pour identifier rapidement les bus, mémoires et points de test critiques [25, 11].

3
Démarche d'analyse technique

3.1 Séquence d'analyse

La démarche est conduite en cinq étapes :

1. collecte d'informations (documentation, certifications, brevets, retours terrain) ;
2. acquisition de plusieurs exemplaires de la cible ;
3. ouverture et caractérisation physique du PCB ;
4. identification composants et interfaces ;
5. interfaçage passif puis actif, avec traçabilité des essais.

REQ_METH_02 – Reproductibilité des analyses

Chaque étape d'analyse doit être documentée dans un journal technique : version matérielle analysée, outils utilisés, conditions d'essai, résultats obtenus et limites observées. Les captures (bus, dumps, photographies) sont horodatées et rattachées à l'échantillon.

- Niveau d'attaquant minimal : **AVA_VAN.Basic**.
- Menace ciblée : **T03** et **T05**.
- La reproductibilité est nécessaire pour distinguer une faiblesse structurelle d'un artefact de manipulation et pour piloter les corrections.
- Références : CERT/CC Vulnerability Notes (méthodologie de documentation), CERT-FR recommandations de durcissement [9, 2].

État de l'art des attaques. Les travaux de rétro-ingénierie de firmware montrent qu'un protocole d'essai non reproductible masque les vecteurs réels d'injection et retarde la correction des failles [11, 24].

4

Protection contre l'accès physique non autorisé

4.1 Étude des solutions d'autoprotection

Les mécanismes observés dans le support ANSSI se regroupent en trois familles :

- **Scellés et dispositifs passifs** : étiquettes, scellés plastiques, scellés métalliques, vis propriétaires, colles structurelles ;
- **Détection active** : capteurs d'ouverture, luminosité, proximité, boucle conductive et logique d'alarme ;
- **Réaction active** : effacement SRAM, invalidation de secrets, blocage de fonctions critiques, passage en mode dégradé.

4.2 Limites des protections passives

Les scellés passifs retardent et mettent en évidence l'ouverture, mais peuvent être contournés (solvants, température, remplacement, impression 3D). Ils restent pertinents pour des contextes de maintenance contrôlée, mais ne suffisent pas pour des actifs critiques.

REQ_PHY_10 – Dispositif passif minimal

Tout équipement doit combiner au moins deux mécanismes passifs différents : un mécanisme anti-ouverture (vis/scellé) et un mécanisme anti-substitution (identifiant unique, marquage inviolable ou équivalent). Les procédures de maintenance doivent vérifier systématiquement ces indicateurs.

- Niveau d'attaquant minimal : **AVA_VAN.Enhanced-Basic**.
- Menace ciblée : **T01**.
- La défense en profondeur réduit les contournements simples et augmente la probabilité de détection d'une compromission physique.
- Références : BSI IT-Grundschutz (mesures organisationnelles et techniques), cadre BSI 200-1/200-2/200-3 et retours d'attaque physique par solvants/chaleur observés en contexte embarqué [8, 5, 6, 7].

État de l'art des attaques. La littérature sur la résistance à la falsification et la substitution physique montre qu'un mécanisme passif unique est contournable avec des moyens de laboratoire standards [1, 25].

4.3 Durcissement du PCB contre l'accès physique local

Le routage et le placement des interfaces sur la carte influencent directement le coût d'une attaque matérielle. Trois leviers complémentaires sont recommandés : enfouissement des pistes critiques, dispersion des points d'accès physiques (connecteurs et points de test) et préférence pour des boîtiers rendant la sonde directe plus coûteuse sur les composants critiques.

REQ_PHY_11 – Enfouissement des pistes sensibles

Les pistes transportant des secrets, des signaux de démarrage sécurisé ou des bus d'administration doivent être routées majoritairement en couches internes, avec limitation stricte des segments accessibles en couche externe. Les vias de transition de ces signaux doivent être protégés (microvias, vias bouchés/masqués ou solution équivalente) afin de réduire les points d'accroche pour micro-sonde.

- Niveau d'attaquant minimal : **AVA_VAN.Moderate**.
- Menace ciblée : **T02** et **T05**.
- L'enfouissement augmente la difficulté de repérage et d'instrumentation des bus critiques, et allonge le temps nécessaire à l'attaque.
- Références : IPC-2221 (routage multicouche), IPC-4761 (protection des vias), état de l'art sur la résistance à la manipulation physique [14, 13, 1].

État de l'art des attaques. Les attaques semi-invasives et de micro-sondage ciblent en priorité les signaux accessibles en surface ; la réduction des zones externes observables augmente significativement le coût d'instrumentation [3, 1].

REQ_PHY_12 – Dispersion des connecteurs et points de test

Les connecteurs de service, pads de test et points de mesure ne doivent pas former une zone compacte unique permettant un accès simultané simple. Leur dispersion géographique sur le PCB, combinée à des signaux de référence non triviales et à des marquages non explicites en production, doit rendre l'interfaçage offensif plus long et plus détectable.

- Niveau d'attaquant minimal : **AVA_VAN.Moderate**.
- Menace ciblée : **T03** et **T05**.
- La dispersion limite la capacité à brancher rapidement des outils de capture et d'injection multi-signaux sur un seul montage.
- Références : CWE-1191/CWE-1244 (exposition debug), retours d'attaques embarquées sur interfaces accessibles [20, 21, 24].

État de l'art des attaques. Les campagnes d'exploitation matérielle montrent qu'une zone de test centralisée (UART/JTAG/SPI regroupés) réduit fortement la barrière d'entrée et accélère les bypass de protections logicielles [24, 19].

REQ_PHY_13 – Usage prioritaire du BGA pour composants critiques

Pour les composants critiques (SoC principal, mémoire de secrets, élément sécurisé), l'usage d'un boîtier **BGA** doit être privilégié par rapport aux boîtiers à pattes exposées (QFP/QFN/TSSOP), sauf contrainte industrielle documentée. En cas de non-usage du BGA, une justification technique doit démontrer un niveau de résistance équivalent vis-à-vis du probing et du rework.

- Niveau d'attaquant minimal : **AVA_VAN.High**.
- Menace ciblée : **T02** et **T05**.
- Le BGA réduit l'accessibilité directe des signaux et impose des opérations de rework plus complexes pour l'attaque (dépose, rebillage, interposition).
- Références : recommandations de résistance à la manipulation physique, classes d'attaques par faute/probing [1, 3].

État de l'art des attaques. Les attaquants peuvent contourner un BGA avec des moyens avancés, mais le coût (équipement, compétence, taux d'échec) est supérieur à celui requis pour des boîtiers à broches exposées ; cette hausse de coût est recherchée pour déplacer l'attaque vers des profils AVA_VAN élevés [1, 25].

4.4 Détection et réaction actives

Les solutions actives exigent une alimentation autonome, une chaîne de décision sûre et des tests périodiques. Elles sont prioritaires lorsque la confidentialité des secrets est critique ou lorsque l'équipement opère hors contrôle physique permanent.

REQ_PHY_20 – Détection active et réaction sécurisée

Pour tout actif de niveau critique, le produit doit implémenter : (i) détection électronique d'ouverture/capteur, (ii) génération d'un événement de sécurité non répudiable, (iii) réaction automatique en moins de 100 ms menant à l'invalidation des matériaux secrets exposés en RAM ou dans un élément sécurisé.

- Niveau d'attaquant minimal : **AVA_VAN.High**.
- Menace ciblée : **T01** et **T02**.
- Une réaction rapide limite la fenêtre d'exfiltration lors d'une ouverture contrainte ou d'une sonde intrusive sur la carte.
- Références : NIST SP 800-193 (protection, detection, recovery), classes CWE matériel pour debug physique [23, 20, 21].

État de l'art des attaques. Les attaques par faute et les attaques semi-invasives illustrent qu'en l'absence de détection/réaction rapide, l'extraction de secrets devient praticable en laboratoire [3, 15].

4.5 Schéma 2 – Détection active et réaction

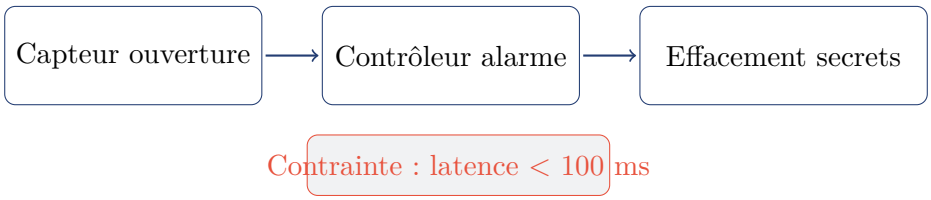


FIGURE 4.1 – Séquence type de détection active d'ouverture.

5
Identification des composants et des interfaces

5.1 Composants prioritaires

L'analyse cible en priorité : mémoires série/parallèle, processeur principal, contrôleurs de communication, coprocesseurs cryptographiques et points de test exposés.

5.2 Interfaces à risque

Les interfaces suivantes doivent être qualifiées : UART, I2C, SPI, JTAG, USB/DFU, ports constructeur, pads de test, ainsi que les alimentations de service susceptibles d'activer des modes cachés.

REQ_IF_30 – Maîtrise des interfaces de debug

Les interfaces de debug et de test en production doivent être désactivées par défaut. Toute réactivation doit être conditionnée à un mécanisme d'authentification forte, temporaire et journalisé.

- Niveau d'attaquant minimal : **AVA_VAN.Moderate**.
- Menace ciblée : **T03**.
- Les retours d'expérience montrent que JTAG/UART actifs constituent une porte d'entrée immédiate vers l'exécution privilégiée.
- Références : CWE-1191 et CWE-1244 (interfaces debug), exemple CVE-2019-18827 (bypass secure boot via accès JTAG précoce) [20, 21, 19].

État de l'art des attaques. Des démonstrations publiques ont montré que l'accès debug en production permet bypass secure boot, dump mémoire et exécution de code non signé [24, 19].

6

Interfaçage et attaques sur le logiciel embarqué

6.1 Interfaçage passif et actif

L'interfaçage passif (oscilloscope, analyseur logique, décodeur protocolaire) permet de comprendre les séquences d'échange sans modifier le comportement. L'interfaçage actif (MITM, usurpation de source, injection) sert à vérifier la robustesse des contrôleurs de communication et des protocoles applicatifs.

6.2 Mise à jour et surfaces logiques

Les mécanismes de mise à jour, notamment DFU et modes usine, constituent une surface d'attaque majeure. Leur exposition doit être réduite et strictement contrôlée en exploitation.

REQ_SW_40 – Chaîne de mise à jour authentifiée

Le mécanisme de mise à jour doit vérifier signature, version et politique anti-retour arrière avant installation. Les clés de vérification sont ancrées dans un composant non réécrivable (fuse, élément sécurisé ou équivalent).

- Niveau d'attaquant minimal : **AVA_VAN.Moderate**.
- Menace ciblée : **T04**.
- La mise à jour non authentifiée permet l'introduction durable d'un firmware malveillant avec persistance après redémarrage.
- Références : NIST SP 800-147 (firmware update), NIST SP 800-193 (résilience du firmware) [22, 23].

État de l'art des attaques. Les compromis de chaînes de mise à jour embarquées et les démonstrations en conférence offensive montrent qu'un contrôle faible de l'authenticité/version ouvre la voie à une prise de contrôle persistante [16, 4, 11].

7

Racine de confiance et Secure Boot

7.1 Secure Boot bout en bout

Le secure boot ne se limite pas au premier chargeur. La vérification d'intégrité et d'authenticité doit couvrir la chaîne complète : ROM de démarrage, bootloader stage 1, bootloader stage 2, noyau, firmwares de coprocesseurs et composants privilégiés.

FIGURE 7.1 – Chaîne de confiance secure boot (inspirée des slides de boot stages).

REQ_ROOT_50 – Vérification continue de la chaîne de boot

Chaque étape de boot doit vérifier cryptographiquement l'étape suivante, avec refus explicite d'exécution en cas d'échec. Les décisions de démarrage doivent être journalisées dans un événement exploitable par la supervision.

- Niveau d'attaquant minimal : **AVA_VAN.High**.
- Menace ciblée : **T04**.
- La rupture d'un maillon de la chaîne de confiance annule le bénéfice du secure boot et ouvre la voie à une compromission persistante.
- Références : NIST SP 800-193, NIST SP 800-147 [23, 22].

État de l'art des attaques. Les bypass de secure boot documentés en conférences techniques confirment qu'un seul maillon non vérifié suffit pour exécuter un code arbitraire dès le démarrage [4, 24].

7.2 TPM, HSE et immuabilité de la racine de confiance

Une chaîne secure boot robuste repose sur une racine de confiance difficile à modifier hors processus contrôlé. Cette racine peut être implantée dans une ROM matérielle immutable, dans un composant TPM, dans un HSE (Hardware Security Engine) intégré au SoC, ou dans un élément sécurisé dédié selon l'architecture de l'équipement. L'objectif n'est pas la technologie pour elle-même, mais la garantie que les clés et les décisions de vérification ne peuvent pas être altérées par une mise à jour non autorisée.

REQ_ROOT_60 – Immuabilité de la racine de confiance

La racine de confiance du secure boot (code d'ancrage, clé(s) racine(s), politique de vérification) doit être stockée dans un mécanisme immuable ou équivalent en résistance à la modification (ROM/fuse, TPM, HSE ou élément sécurisé). Toute évolution de cette racine doit être soumise à une procédure de transition de clé explicitement autorisée, tracée et auditable.

- Niveau d'attaquant minimal : **AVA_VAN.High**.
- Menace ciblée : **T04**.
- Une racine modifiable sans contrôle annule la chaîne de confiance, même si les étapes de boot suivantes vérifient des signatures.
- Références : NIST SP 800-193 (roots of trust, protection/recovery) [23].

État de l'art des attaques. Les attaques par faute et par contournement de vérification montrent qu'une racine de confiance mutable est un point de rupture critique pour l'ensemble du démarrage sécurisé [3, 4].

REQ_ROOT_70 – Usage prioritaire des briques matérielles disponibles

Lorsque l'équipement intègre une brique de sécurité exploitable pour le secure boot (ex. TPM, HSE, mécanisme constructeur équivalent), cette brique doit être utilisée en priorité pour l'ancrage des clés, l'attestation de l'état de boot ou la vérification cryptographique des étapes critiques, dès lors qu'elle est éligible fonctionnellement.

- Niveau d'attaquant minimal : **AVA_VAN.Moderate** à **AVA_VAN.High**.
- Menace ciblée : **T04** et **T05**.
- L'usage effectif des mécanismes matériels disponibles réduit l'exposition des secrets et des décisions de vérification dans des zones logicielles plus faciles à compromettre.
- Références : NIST SP 800-193 (device roots of trust) [23].

État de l'art des attaques. L'extraction de secrets par canaux auxiliaires et faute est significativement facilitée lorsque les clés restent dans des composants généralistes sans ancrage matériel dédié [15, 3].

REQ_ROOT_80 – Technologie de remplacement à niveau équivalent

Si TPM/HSE ne sont pas disponibles ou non éligibles sur l'équipement, l'implémentation doit utiliser une technologie alternative offrant un niveau de sécurité similaire (par exemple élément sécurisé dédié), avec justification documentée de l'équivalence sur la protection des clés, la résistance à la modification et la robustesse des opérations cryptographiques.

- Niveau d'attaquant minimal : **AVA_VAN.High**.
- Menace ciblée : **T04** et **T05**.
- Le recours à une alternative explicite et justifiée évite les dégradations implicites de sécurité lors des variations de plateforme matérielle.
- Références : NIST SP 800-193 et bonnes pratiques CERT/CC [23, 9].

État de l'art des attaques. De nombreux cas de terrain montrent qu'un remplacement non maîtrisé des mécanismes de confiance dégrade la résistance aux attaques physiques, aux fautes et à l'extraction de clés [25, 3].

REQ_ROOT_90 – Suivi sécurité des logiciels résidents constructeur

Le fabricant de l'équipement doit maintenir un suivi de sécurité explicite des logiciels résidents fournis par le constructeur de composants (ex. BootROM, moniteurs de sécurité, microcodes et firmwares de démarrage OEM), au même niveau d'exigence que le logiciel applicatif. Ce suivi inclut : (i) veille CVE/advisories, (ii) évaluation d'exposition du produit, (iii) plan de mitigation lorsque le correctif n'est pas déployable (contournement, durcissement de configuration, restriction d'usage, remplacement matériel), (iv) traçabilité MCO/MCS des décisions.

- Niveau d'attaquant minimal : **AVA_VAN.High**.
- Menace ciblée : **T04** et **T05**.
- Les composants logiciels résidents du fabricant sont des cibles d'attaque au même titre que le firmware applicatif ; l'absence de suivi crée une dette de sécurité durable sur des briques parfois non patchables.
- Références : NIST SP 800-193 (résilience et recovery), cas CVE sur BootROM i.MX6 et Tegra [23, 17, 18].

État de l'art des attaques. Le bypass de vérification de signature sur la BootROM de la famille i.MX (incluant i.MX6) [17] et la classe d'attaques Fusée Gelée sur Tegra (documentée publiquement sur Tegra X1) [12, 18] illustrent que les logiciels résidents constructeur doivent faire l'objet d'un suivi de sécurité continu, au même titre que le logiciel applicatif.

Bibliographie

[1] Ross Anderson and Markus Kuhn. Tamper resistance – a cautionary note. In *Proceedings of the 2nd USENIX Workshop on Electronic Commerce*, pages 1–11. USENIX Association, 1996.

[2] ANSSI. Cert-fr : Alertes, avis et recommandations. CERT-FR Portal, 2026. Accessed 2026-05-31.

[3] Alessandro Barenghi, Luca Breveglieri, Israel Koren, and David Naccache. Fault injection attacks on cryptographic devices : Theory, practice, and countermeasures. *Proceedings of the IEEE*, 100(11) :3056–3076, 2012.

[4] Yuriy Bulygin and Oleksandr Furtak. A tale of one software bypass of windows 8 secure boot. Black Hat USA, 2014.

[5] Bundesamt fuer Sicherheit in der Informationstechnik. Bsi standard 200-1 : Information security management systems (isms). Technical report, BSI, 2017.

[6] Bundesamt fuer Sicherheit in der Informationstechnik. Bsi standard 200-2 : It-grundschutz methodology. Technical report, BSI, 2017.

[7] Bundesamt fuer Sicherheit in der Informationstechnik. Bsi standard 200-3 : Risk analysis based on it-grundschutz. Technical report, BSI, 2017.

[8] Bundesamt fuer Sicherheit in der Informationstechnik. It-grundschutz compendium. BSI Web Portal, 2026. Accessed 2026-05-31.

[9] CERT Coordination Center. Vulnerability notes database. CERT/CC Knowledge Base, 2026. Accessed 2026-05-31.

[10] Common Criteria Development Board. Common criteria for information technology security evaluation, part 3 : Security assurance components. Common Criteria Portal, 2022. AVA_VAN levels : Basic, Enhanced-Basic, Moderate, High.

[11] Andrei Costin, Apostolis Zarras, and Aurelien Francillon. A large-scale analysis of the security of embedded firmwares. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 95–110, 2014.

[12] fail0verflow. Shofel2, a tegra x1 and nintendo switch exploit. Technical disclosure / exploit write-up, 2018. Attaque de type Fusée Gelée sur Tegra X1 (BootROM/RCM).

[13] IPC. Ipc-4761 : Design guide for protection of printed board via structures. Industry Standard, 2017.

[14] IPC. Ipc-2221 : Generic standard on printed board design. Industry Standard, 2021.

[15] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in Cryptology – CRYPTO'99*, pages 388–397. Springer, 1999.

[16] Charlie Miller and Chris Valasek. Remote exploitation of an unaltered passenger vehicle. Black Hat USA, 2015.

[17] MITRE. Cve-2017-7932. Common Vulnerabilities and Exposures, 2017. NXP i.MX family : bypass de verification de signature via certificat forge.

[18] MITRE. Cve-2018-6242. Common Vulnerabilities and Exposures, 2018. NVIDIA Tegra BootROM RCM buffer overflow permettant l'execution de code non verifie.

[19] MITRE. Cve-2019-18827. Common Vulnerabilities and Exposures, 2019.

[20] MITRE. Cwe-1191 : On-chip debug and test interface with improper access control. Common Weakness Enumeration, 2026. Accessed 2026-05-31.

[21] MITRE. Cwe-1244 : Internal asset exposed to unsafe debug access level or state. Common Weakness Enumeration, 2026. Accessed 2026-05-31.

[22] National Institute of Standards and Technology. Bios protection guidelines. Technical Report SP 800-147, NIST, 2011.

[23] National Institute of Standards and Technology. Platform firmware resiliency guidelines. Technical Report SP 800-193, NIST, 2018.

[24] Johannes Obermaier and Florian Tatschner. Shedding too much light on a microcontroller's firmware protection. In *12th USENIX Workshop on Offensive Technologies (WOOT 18)*, 2018.

[25] Mohammad Tehranipoor and Farinaz Koushanfar. A survey of hardware trojan taxonomy and detection. *IEEE Design & Test of Computers*, 27(1) :10–25, 2010.

Licence