Approche automatisée pour l'évaluation des risques des mises à jour OTA dans les véhicules définis par logiciel

Khaoula Sghaier, Ghada Gharbi, Badis Hammi, Pierre Merdrignac, Pierre Parrend, Didier Verna

Approche automatisée pour l'évaluation des risques des mises à jour OTA dans les véhicules définis par logiciel

Khaoula Sghaier[1,2,3], Ghada Gharbi[1], Badis Hammi[3], Pierre Merdrignac[2], Pierre Parrend[1,4], and Didier Verna[1]

[1]LRE, EPITA, 14-16 Rue Voltaire, Le Kremlin-Bicêtre, France
[2]VEDECOM, 23 bis Allée des Marronniers, Versailles, France
[3]SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris, Palaiseau, France
[4]Université de Strasbourg, CNRS, ICube, UMR 7357, Strasbourg, France

Résumé

Les mises à jour logicielles à distance (OTA) dans les véhicules définis par logiciel (SDVs) introduisent des risques majeurs de sécurité et de sûreté, en raison de leur capacité à impacter des fonctions critiques et à se propager à l'échelle de flottes entières.

Ce travail propose un framework automatisé et adaptatif d'évaluation des risques OTA, combinant de manière holistique les méthodes TARA, HARA et DREAD afin d'intégrer simultanément les dimensions de cybersécurité, de sûreté fonctionnelle et d'impact systémique. À partir d'une description en langage naturel d'une vulnérabilité et de la criticité de la mise à jour, le framework génère en quelques secondes des scores de risque contextualisés.

Véhicules définis par logiciel (SDV), mises à jour à distance (OTA), évaluation des risques, analyse de vulnérabilités

1 Introduction

Les véhicules définis par le logiciel (Software-Defined Vehicles, SDVs) placent le logiciel au cœur des fonctionnalités et des mécanismes de sécurité

du véhicule [1]. Cette évolution repose sur des mises à jour logicielles Over-The-Air (OTA) fréquentes, couvrant des systèmes de criticité hétérogène, du non critique aux fonctions de sécurité telles que la conduite autonome ou le freinage [2, 3].

L'évaluation des risques associés aux mises à jour à OTA dans les SDVs soulève plusieurs défis majeurs. Une même mise à jour peut impacter plusieurs calculateurs électroniques (ECU) présentant des niveaux de criticité distincts [4, 22]. Plusieurs travaux ont démontré la possibilité d'exploiter à distance des systèmes initialement non critiques pour atteindre des ECUs sensibles, notamment sur un Tesla Model 3 [7]. Par ailleurs, la complexité croissante des architectures SDV, fondées sur des plateformes de calcul partagées et hautes performances, accroît significativement la surface d'attaque [5]. Enfin, le déploiement massif et simultané des mises à jour OTA introduit un risque systémique, où une compromission unique peut affecter instantanément une flotte entière de véhicules [6].

Face à ces enjeux, les méthodologies d'évaluation des risques existantes présentent des limites : TARA (ISO/SAE 21434) se concentre sur la cybersécurité [10], tandis que HARA (ISO 26262) traite la sûreté fonctionnelle sans intégrer les menaces cyber [11]. Les approches hybrides, telles que HATARA [12], restent largement manuelles et peu adaptées aux vecteurs d'attaque et aux dynamiques de propagation propres aux mises à jour OTA.

Pour répondre à ces limitations, cet article propose un framework automatisé combinant de manière adaptative TARA, HARA et DREAD afin de fournir une évaluation holistique et contextualisée des risques OTA dans les SDV.

2 Background

Nous rappelons ici les principes fondamentaux des méthodes d'analyse de risque TARA, HARA et DREAD ainsi que la base de données ATD.

2.1 TARA

La méthode TARA (Threat Analysis and Risk Assessment), normalisée par l'ISO/SAE 21434, quantifie le risque cybersécurité d'une vulnérabilité en combinant son impact sur quatre domaines - sûreté fonctionnelle, financier, opérationnel et vie privée - avec une estimation de la faisabilité d'attaque dérivée des métriques CVSS v3.1 [27, 28] :

$$S_{\text{TARA}} = 1 + (\text{Impact} \times \text{Feasibility}) \tag{1}$$

où l'évaluation combinée de l'**impact** couvre quatre aspects, chacun noté $\in \{1, 2, 3, 4\}$: sûreté fonctionnelle, financier, ppérationnel et cie privée.
La faisabilité d'attaque est estimée à partir du score d'exploitabilité CVSS :

$$E = 8.22 \times V \times C \times P \times U \tag{2}$$

avec E l'exploitabilité, V le vecteur d'attaque, C la complexité d'attaque, P les privilèges requis et U l'interaction utilisateur. La correspondance entre score d'exploitabilité et niveau de faisabilité est établie selon le standard ISO/SAE 21434 (Tab. 1).

TABLE 1 – Tableau de correspondance de l'exploitabilité CVSS

Niveau de faisabilité d'attaque	**Valeur d'exploitabilité CVSS**
Élevé	2,96 – 3,89
Moyen	2,00 – 2,95
Faible	1,06 – 1,99

2.2 HARA

La méthode HARA (Hazard Analysis and Risk Assessment), définie par la norme ISO 26262, évalue les implications de sûreté fonctionnelle d'une situation dangereuse en déterminant le niveau d'intégrité de sécurité automobile (ASIL) requis à partir de trois paramètres opérationnels [4] :

$$\text{ASIL} = f(S, E, C) \tag{3}$$

où :
— $S \in \{S0, S1, S2, S3\}$: Sévérité - gravité potentielle des blessures
— $E \in \{E0, E1, E2, E3, E4\}$: Exposition - probabilité d'occurrence de la situation opérationnelle dangereuse
— $C \in \{C0, C1, C2, C3\}$: Contrôlabilité - capacité du conducteur à éviter le dommage.

Le niveau ASIL résultant est défini sur l'échelle :

$$\text{ASIL} \in \{QM, A, B, C, D\} \tag{4}$$

où QM (Quality Management) indique l'absence d'exigence de sûreté, et D représente le niveau de criticité le plus élevé. Sa détermination repose sur la matrice de risque tridimensionnelle spécifiée par l'ISO 26262-3.

2.3 DREAD

Le modèle DREAD est un système de scoring qualitatif destiné à estimer l'impact potentiel d'une vulnérabilité exploitée. Dans sa formulation originale, il agrège cinq paramètres : Damage (D), Reproducibility (R), Exploitability (E), Affected users (A) et Discoverability (D).

$$S_{\text{DREAD}} = \frac{D + R + E + A + D}{5} \tag{5}$$

2.4 Automotive Threat Database (ATD)

L'Automotive Threat Database (ATD) [21] est une base de connaissances ouverte recensant des incidents de cybersécurité automobile documentés dans le monde réel. Chaque entrée de la base structure un incident selon un ensemble de champs normalisés : vecteur d'attaque, composant ciblé, impact fonctionnel, métriques CVSS associées, ainsi qu'une description textuelle de la vulnérabilité et de ses conditions d'exploitation.

3 Etat de l'art

L'évaluation des risques dans le domaine automobile a connu une évolution significative avec les véhicules connectés, en raison de l'augmentation exponentielle de la complexité logicielle et de l'élargissement des vecteurs d'attaque potentiels.

TARA traditionnelle, normalisée dans ISO/SAE 21434 [10], traite la cybersécurité en modélisant le risque selon une formulation quantitative du type R = 1 + (Impact × Faisabilité), où l'Impact englobe les aspects Sécurité, Financier, Opérationnel et Protection de la vie privée, tandis que la Faisabilité repose sur l'évaluation de la complexité d'attaque selon les métriques CVSS. [16].

D'autres méthodes comme TVRA [17] et EVITA [23] se concentrent sur la sécurité mais ne couvrent pas les vecteurs d'attaque spécifiques aux architectures OTA distribuées (serveur cloud, edge, véhicule). Les approches faisant le pont entre sûreté et sécurité telles que HATARA [13], HEAVENS [20], SAHARA [19], et ACTISM [18] offrent une couverture plus complète mais restent confinées à la phase de conception et manquent d'automatisation pour l'évaluation en temps réel des mises à jour OTA.

Notre approche est la première méthodologie ciblant les mises à jour OTA dans les SDVs, intégrant la veille dynamique sur les menaces, l'impact à l'échelle de la flotte, et l'évaluation des vulnérabilités en temps réel.

4 Positionnement dans le pipeline OTA

Notre framework intègre de manière holistique les trois méthodologies présentées - TARA, HARA et DREAD - au sein d'un pipeline d'évaluation automatisé et adaptatif.

L'automatisation repose sur un moteur de correspondance sémantique : à partir d'une description en langage naturel d'une vulnérabilité OTA, un modèle de transformers (all-MPNet-base-v2, embeddings de dimension 768) calcule la similarité cosinus entre cette description et l'ensemble des entrées de l'Automotive Threat Database (ATD). L'entrée la plus proche sémantiquement est sélectionnée, et ses champs structurés - vecteur d'attaque, métriques CVSS, composant ciblé, impact fonctionnel - sont extraits pour alimenter directement les trois composantes d'évaluation, sans intervention manuelle.

Chaque composante couvre une dimension distincte du risque : TARA quantifie l'exposition cybersécurité via les métriques d'exploitabilité CVSS et l'impact sur quatre domaines critiques ; HARA détermine le niveau ASIL requis à partir des paramètres de sûreté fonctionnelle ISO 26262 ; DREAD estime l'impact potentiel à l'échelle de la flotte. Pour cette dernière composante, les paramètres Reproducibility, Exploitability et Discoverability sont écartés, leurs dimensions étant déjà capturées par la composante TARA - seuls Damage et Affected users sont retenus, préservant ainsi l'orthogonalité du score composite.

Cette perspective intégrée est particulièrement cruciale dans les systèmes automobiles, où une compromission cybersécurité peut déclencher des défaillances de sûreté fonctionnelle, transformant une vulnérabilité logicielle en risque direct pour la sécurité des passagers [24, 25].

Fig. 1 présente l'intégration du pipeline d'évaluation des risques proposé dans l'architecture OTA. Lorsqu'une vulnérabilité zero-day est identifiée dans n'importe quel composant (e.g., nœud edge) via des mécanismes de surveillance ou d'analyse comportementale, elle est immédiatement signalée au serveur du constructeur. À réception, un processus automatisé d'évaluation des risques est déclenché, générant des scores de risque quantitatifs utilisant des méthodologies complémentaires : TARA, HARA et DREAD.

L'écart temporel entre la découverte d'une vulnérabilité et la disponibilité du correctif représente une fenêtre d'exposition critique durant laquelle les véhicules demeurent susceptibles d'exploitation. Pour traiter cette fenêtre, notre framework opère de manière proactive en évaluant le niveau de risque en fonction des conditions opérationnelles spécifiques à chaque mise à jour OTA. Cette évaluation en temps réel permet l'activation de contrôles de sécurité compensatoires et de mesures défensives proportionnelles au ni-

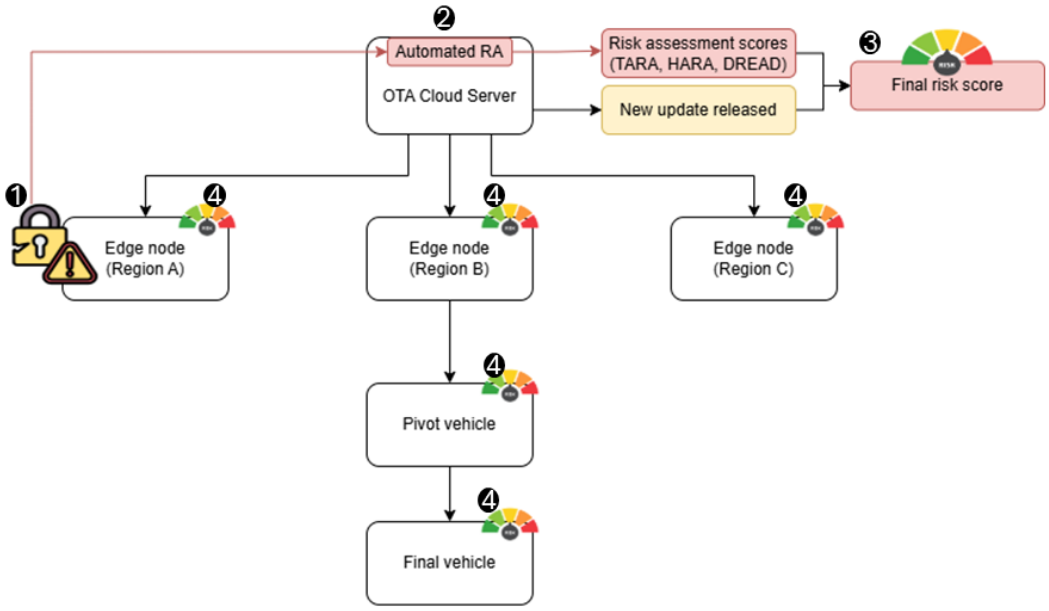

FIGURE 1 – Pipeline d'évaluation automatisée des risques dans l'architecture OTA

veau de risque calculé, atténuant ainsi l'exposition aux attaques potentielles avant le déploiement du correctif.

Lors de la publication d'un correctif, le module d'évaluation est mis à jour dynamiquement pour refléter la réduction de la surface d'attaque consécutive au déploiement du patch. Les mécanismes de défense en profondeur désormais en place conduisent à un score de risque global recalculé et plus faible, qui est propagé à travers l'ensemble des composants architecturaux OTA. Le système ajuste ainsi sa posture de sécurité de manière adaptative, garantissant des mesures de protection proportionnées sans surcharge computationnelle inutile.

4.1 Aspect dynamique

La capacité dynamique du framework traite la nature évolutive des menaces de cybersécurité automobile par intégration continue avec des bases de données de threat intelligence en temps réel. Le framework s'adapte automatiquement à :

— **Vulnérabilités zero-day** : à la découverte d'une vulnérabilité zero-day, le moteur de correspondance sémantique les incorpore sans reconfiguration manuelle. L'espace d'embedding basé sur des transformers positionne automatiquement les nouvelles menaces par rapport aux motifs d'attaque existants.

— **Techniques de sécurité émergentes** : l'approche proposée s'appuie sur une réévaluation continue des scores de risque qui reflète l'évolution du contexte de sécurité en fonction des vulnérabilités résiduelles et des patches déployés. Cette traçabilité quantitative du niveau de risque au fil du cycle de vie OTA constitue une avancée par rapport aux évaluations statiques traditionnelles, offrant une visibilité temps réel sur l'efficacité des mesures correctives appliquées.

4.2 Aspect adaptatif

Au-delà de l'adaptation temporelle aux nouvelles menaces, le framework implémente un ajustement adaptatif de la quantification à trois niveaux basés sur les caractéristiques spécifiques de chaque scénario de mise à jour. L'ensemble des coefficients présentés dans cette section est entièrement paramétrable, permettant à chaque OEM d'adapter le framework selon ses politiques de sécurité et ses contraintes opérationnelles spécifiques.

Adaptation contextuelle : le framework emploie une pondération adaptive des trois frameworks de scoring (TARA, HARA, DREAD) selon la

criticité du système :

$$\text{Score}_{\text{risk}} = \alpha S_{\text{TARA}} + \beta S_{\text{HARA}} + \gamma S_{\text{DREAD}} \tag{6}$$

$$(\alpha, \beta, \gamma) = \begin{cases} (0.4,\ 0.4,\ 0.2), & \text{mise à jour non critique,} \\ (0.25,\ 0.5,\ 0.25), & \text{mise à jour critique.} \end{cases} \tag{7}$$

Le score de risque composite intègre de multiples méthodologies d'évaluation par une combinaison linéaire pondérée, où les coefficients de pondération α, β et γ reflètent l'importance relative de chaque méthode pour un contexte de mise à jour donné.

Adaptation de la surface d'attaque : le paramètre "utilisateurs affectés" dans la méthode DREAD est davantage ajusté selon la localisation de la compromission :

— Niveau cloud : impact maximal sur la flotte (élevé)
— Niveau edge : impact régional (modéré)
— Niveau véhicule : impact individuel (faible)

Cette adaptation multidimensionnelle assure qu'une description de vulnérabilité générique produit différents scores de risque selon *ce qui* est mis à jour (domaine ECU), *où* la vulnérabilité est découverte (cloud/edge/véhicule), et *quelle criticité* a la mise à jour OTA, permettant une paramétrisation précise et consciente du contexte des protocoles de sécurité plutôt que des approches statiques.

4.3 Exemple

Pour évaluer notre approche, nous construisons un scénario synthétique inspiré de la vulnérabilité de l'API concessionnaire Kia, divulguée en septembre 2024 [1], dans laquelle un attaquant distant peut exploiter une API backend OEM exposée via le numéro d'identification du véhicule (VIN) pour injecter des commandes ciblant les fonctions d'une flotte de véhicules. Aucun identifiant CVE n'ayant été attribué à cette vulnérabilité, elle est absente de la base ATD.

Le framework retourne l'entrée correspondante ATD-37 / CVE-2023-32156 avec un score de confiance de 0,758. Cette entrée représente un contournement de validation de signature de firmware de passerelle Tesla partageant la même surface d'attaque : accès distant non authentifié à l'infrastructure backend OEM permettant l'exécution de commandes véhicule. Ce résultat

1. https ://samcurry.net/hacking-kia

démontre la capacité du moteur de correspondance sémantique à identifier la menace connue la plus pertinente, capturant l'effet de chaîne d'attaque (*kill chain*) et validant ainsi la généralisation sémantique aux menaces non référencées.

À partir de la description de la vulnérabilité et de l'instance identifiée dans l'ATD, les paramètres sont extraits automatiquement. **TARA** : AV=0,62, AC=0,77, PR=0,62, UI=0,85 $\rightarrow$ exploitabilité = 2,07 (*Low*), impact sévère sur les quatre domaines ; **HARA** : $f(S3, E4, C3) \rightarrow$ ASIL D ; **DREAD** : Damage=10, Affected Users=10. Le score agrégé final s'établit à **4,75/5,0** pour une mise à jour critique, soit un niveau de risque **CRITIQUE**, contre **4,30/5,0** pour une mise à jour non critique, soit un niveau **ÉLEVÉ**. Cette différence illustre la capacité du framework à adapter le score de risque au contexte opérationnel sans modifier les paramètres de la vulnérabilité.

5 Conclusion

Dans ce travail, nous présentons un framework automatisé et adaptatif pour l'évaluation des risques associés aux mises à jour OTA dans les SDVs. S'appuyant sur l'analyse sémantique de sources de threat intelligence et un scoring contextuel, ce framework permet une quantification automatique et structurée des risques, facilitant ainsi la priorisation des menaces et la définition de stratégies d'atténuation proportionnées. Conçu comme un outil d'aide à la décision, il constitue le fondement méthodologique d'une approche plus large visant le développement d'un protocole OTA end-to-end adaptatif, capable d'ajuster dynamiquement les mécanismes cryptographiques et les contrôles de sécurité en fonction du niveau de risque et de la criticité du système.

Remerciements

Badis Hammi a reçu un financement de la Commission européenne dans le cadre du projet Horizon Europe AI4CCAM (convention de subvention n° 101076911).

Références

[1] M. Broy, "Challenges in automotive software engineering," in Proceedings of the 28th International Conference on Software Engineering (ICSE), 2006, pp. 33-42.

[2] A. Macher et al., "A review of automotive software development lifecycle and challenges," IEEE Access, vol. 8, pp. 177487-177503, 2020.

[3] J. Dürrwang et al., "OTA Updates for Connected and Autonomous Vehicles : Current Status and Future Directions," IEEE Communications Surveys & Tutorials, vol. 23, no. 3, pp. 1681-1710, 2021.

[4] ISO 26262-3 :2018, "Road vehicles — Functional safety — Part 3 : Concept phase," International Organization for Standardization, 2018.

[5] S. Fürst and M. Bechter, "AUTOSAR for connected and autonomous vehicles : The AUTOSAR adaptive platform," in 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), 2020, pp. 196-205.

[6] Upstream Security Ltd. (2024). Global Automotive Cybersecurity Report : The Automotive Cybersecurity Inflection Point — From Experimental Hacking to Large-Scale Automotive Attacks, the Focus Shifts to Impact. Upstream Security Ltd., 2024.

[7] K. Jansen et al., "Car Hacking : Accessing and Exploiting the CAN Bus Protocol," in Network Security, 2020, pp. 8-11.

[8] A. Palanca et al., "A systematic review of IoT malware threats and detection mechanisms in edge computing," Journal of Systems Architecture, vol. 128, 2022.

[9] I. Studnia et al., "Survey on security threats and protection mechanisms in embedded automotive networks," in 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W), 2013, pp. 1-12.

[10] ISO/SAE 21434 :2021, "Road vehicles — Cybersecurity engineering," International Organization for Standardization, 2021.

[11] ISO 26262 :2018, "Road vehicles — Functional safety," International Organization for Standardization, 2018.

[12] G. Macher et al., "A Combined Safety-Hazards and Security-Threat Analysis Method for Automotive Systems," in Computer Safety, Reliability, and Security (SAFECOMP), Lecture Notes in Computer Science, vol. 9337, 2015, pp. 237-250.

[13] Jherrod Thomas. "HATARA : A Novel Approach by Fusion of HARA and TARA for System Safety and Security Analysis." Volume. 9 Issue. 2, February - 2024 International Journal of Innovative Science and Research Technology (IJISRT), www.ijisrt.com. ISSN - 2456-2165, PP :- 381-398.https ://doi.org/10.5281/zenodo.10665073

[14] T. Ruland et al., "Evaluation of Automotive Cybersecurity Risk Assessment Methods," in European Conference on Software Architecture Workshops (ECSAW), 2021, pp. 1-6.

[15] S. Jayaratne et al., "Automotive Threat Database (AutomotiveTD) : A comprehensive collection of real-world automotive cybersecurity incidents," GitHub Repository, 2024. [Online]. Available : https ://github.com/jayaratned/AutomotiveTD

[16] P. Mell et al., "Common Vulnerability Scoring System (CVSS) v3.1 : Specification Document," FIRST.org, 2019.

[17] Mafijul Md. Islam, Aljoscha Lautenbach, Christian Sandberg, and Tomas Olovsson. 2016. A Risk Assessment Framework for Automotive Embedded Systems. In Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security (CPSS '16). Association for Computing Machinery, New York, NY, USA, 3–14. https ://doi.org/10.1145/2899015.2899018

[18] Huang, Shaofei et al. "ACTISM : Threat-informed Dynamic Security Modelling for Automotive Systems." ArXiv abs/2412.00416 (2024) : n. pag.

[19] I. Friedberg et al., "SAHARA : A Security-Aware Hazard and Risk Analysis Method," in IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2017, pp. 621-624.

[20] R. Bloomfield et al., "HEAVENS - A Practical Approach to Automotive Security Analysis," SAE Technical Paper 2016-01-0062, 2016.

[21] Don Nalin Dharshana Jayaratne. jayaratned/AutomotiveTD. Sept. 2024. url : https ://github.com/jayaratned/AutomotiveTD.

[22] Sghaier, Khaoula, et al. "Advancing Security in Software-Defined Vehicles : A Comprehensive Survey and Taxonomy." arXiv preprint arXiv :2510.09675 (2025).

[23] M. Abouelnaga and C. Jakobs, "Security Risk Analysis Methodologies for Automotive Systems," arXiv preprint arXiv :2307.02261, 2023. :contentReference[oaicite :0]index=0

[24] C. Miller, "Lessons learned from hacking a car," in IEEE Design & Test, vol. 36, no. 6, pp. 7-9, Dec. 2019, doi : 10.1109/MDAT.2018.2863106.

[25] Kovacevic, A.; Gligoric, N. Enhancing Security of Automotive OTA Firmware Updates via Decentralized Identifiers and Distributed Ledger Technology. Electronics 2024, 13, 4640. https ://doi.org/10.3390/electronics13234640

[26] Villegas, Mónica M. et Hernán Astudillo (2020). OTA Updates Mechanisms : A Taxonomy and Techniques Catalog. Dans : Actes du XXI Simposio Argentino de Ingeniería de Software (ASSE 2020), 49JAIIO, pp. 139–158. Disponible en ligne : https ://49jaiio.sadio.org.ar/pdfs/asse/ASSE%2008.pdf

[27] ISO/SAE 21434 :2021, *Road vehicles — Cybersecurity engineering*, International Organization for Standardization, 2021.

[28] P. Mell, K. Scarfone et S. Romanosky, *Common Vulnerability Scoring System (CVSS) v3.1 : Specification Document*, FIRST.org, 2019. [En ligne]. Disponible :https ://www.first.org/cvss/specification-document