

DAIMLER TRUCK

**Vers un avenir sûr:
découvrez la cybersécurité
pour les véhicules.**

Juin 2024

Mark Westendorp | Daimler Buses GmbH
mark.westendorp@daimlertruck.com





Qu'est-ce que la cybersécurité ?

Comment nous définissons cyber et cybersécurité?



CYBER désigne l'espace numérique connecté qui comprend les réseaux, les systèmes et la sauvegarde, la présentation et la gestion des informations à l'aide de l'infrastructure informatique.

Cyberattaques

Généralement dans le but **d'accéder à des informations confidentielles, de les modifier ou de les détruire**, d'extorquer des fonds ou de perturber **le fonctionnement normal de l'entreprise**.



Cybersécurité

Comprend des **technologies, des services, des stratégies, des pratiques** et des **directives** pour **protéger les personnes, les données** et les **systèmes techniques** contre un large éventail d'attaques numériques.





Qu'est-ce que la cybersécurité pour les véhicules ?

Qu'est-ce qui différencie la cybersécurité des véhicules de la sécurité fonctionnelle ?



Sécurité fonctionnelle

- Développer et concevoir une fonction de manière à ce qu'elle soit **sûre**
- Progression dans le développement dans le cadre du développement standard prévu



- Le but est de garantir la sécurité des systèmes du véhicule **en évitant les dysfonctionnements ou les défauts susceptibles d'entraîner des accidents ou des dommages.**
- Cela inclut la mise en œuvre de **mécanismes de sécurité et de redondances** pour réduire les risques et maintenir un fonctionnement sûr.

Cybersécurité

- Développer et concevoir l'infrastructure pour qu'elle soit **protégée**
- Le développement est influencé par des influences extérieures (incontrôlable)



- Se concentre sur la protection des systèmes du véhicule **contre l'accès non autorisé, la manipulation ou les perturbations par des intervenants externes.**
- Comprend la mise **en œuvre de protocoles de sécurité, de cryptage et de mécanismes d'authentification** pour protéger les fonctions et les données du véhicule.



Pourquoi la cybersécurité des véhicules est-elle si importante ?



Bien que les futures architectures électroniques EE puissent contenir moins de calculateurs, le nombre de lignes de code continuera d'augmenter

L'espace numérique dans le véhicule moderne ne cesse de croître



Puissance de calcul de 20 ordinateurs

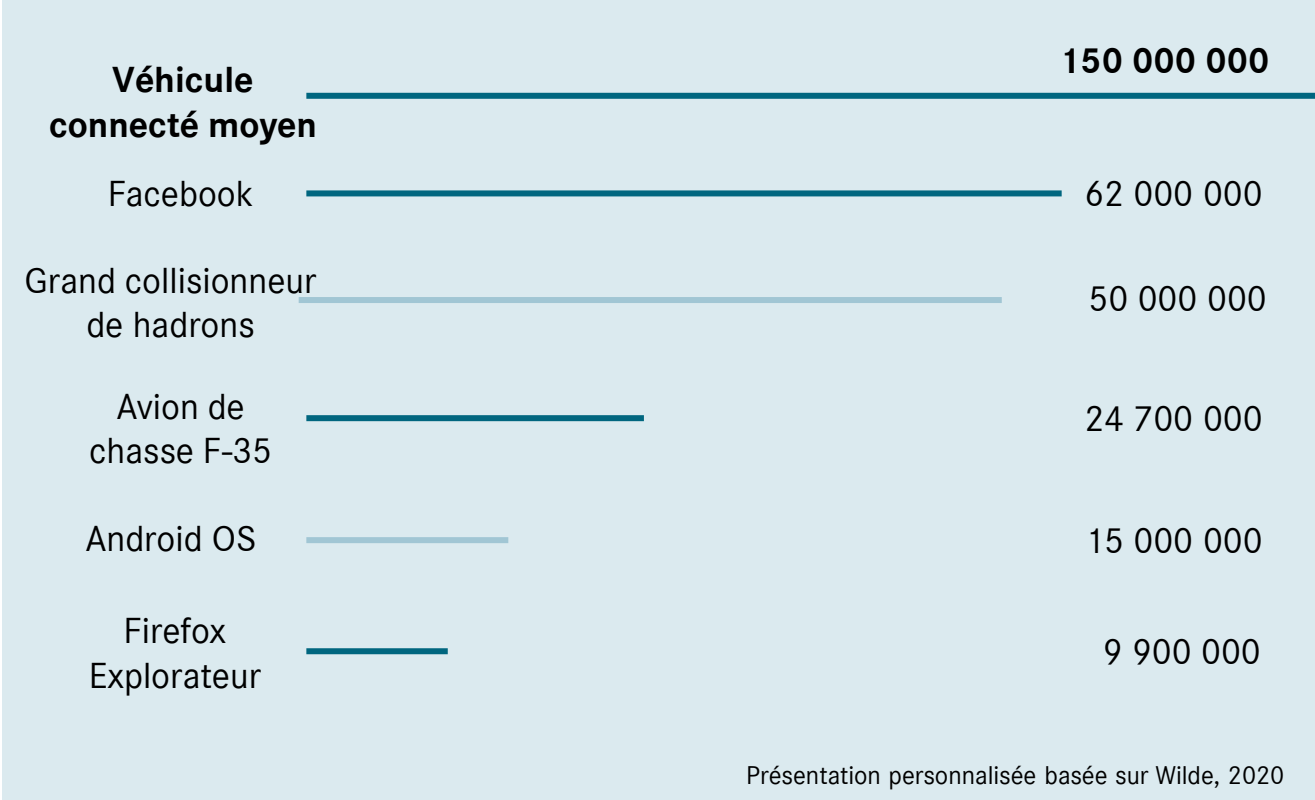


150 millions de lignes de code logiciel



Traite jusqu'à 25 giga-octets de données par heure

Charette, 2022





Qu'est-ce que la norme UNECE R155 ?

Qu'est-ce que le règlement UNECE R155 ?



Le règlement sur la cybersécurité de l'ONU-CEE en bref

Qui?



- Le **WP.29*** fait partie de la UNECE
- Sa mission consiste à **harmoniser les réglementations automobiles dans le monde entier et à développer des réglementations techniques** pour la sécurité des véhicules, la protection de l'environnement et l'efficacité énergétique

Quoi?



- Le R155 est **une norme réglementaire** pour la **cybersécurité** du véhicule
- WP.29 **surveille le développement et la mise en œuvre du règlement CEE-ONU R155** et assure l'harmonisation globale des normes

Où?



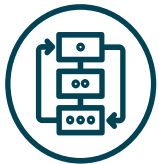
- Le règlement s'applique aux **véhicules immatriculés dans des pays** qui reconnaissent **les réglementations UN-ECE**, y compris R155 : le **pays de vente/d'exportation** est déterminant
- **Sécurité : l'Europe**, mais aussi d'autres pays en dehors de l'Europe adaptent la R155**
- **Le nombre de pays concerné évolue de manière dynamique**

Quel est l'impact du règlement UNECE R155 sur les constructeurs ?



Le règlement UNECE R155 entre en vigueur en juillet 2024
pour toutes les nouvelles immatriculations

Procédure



CSMS

§

Certification

Contrôle annuel des documents requis
Recertification tous les trois ans

Aspect technique



**Réception
par type**

§

**Une certification de la
technologie de sécurité du
véhicule** est nécessaire pour tous
les modèles de véhicule

CSMS : Système de gestion de la cybersécurité

Quelles sont les exigences du nouveau règlement ?



Créer un cadre complet pour **identifier, évaluer et gérer les risques de cybersécurité** tout au long du cycle de vie du véhicule.

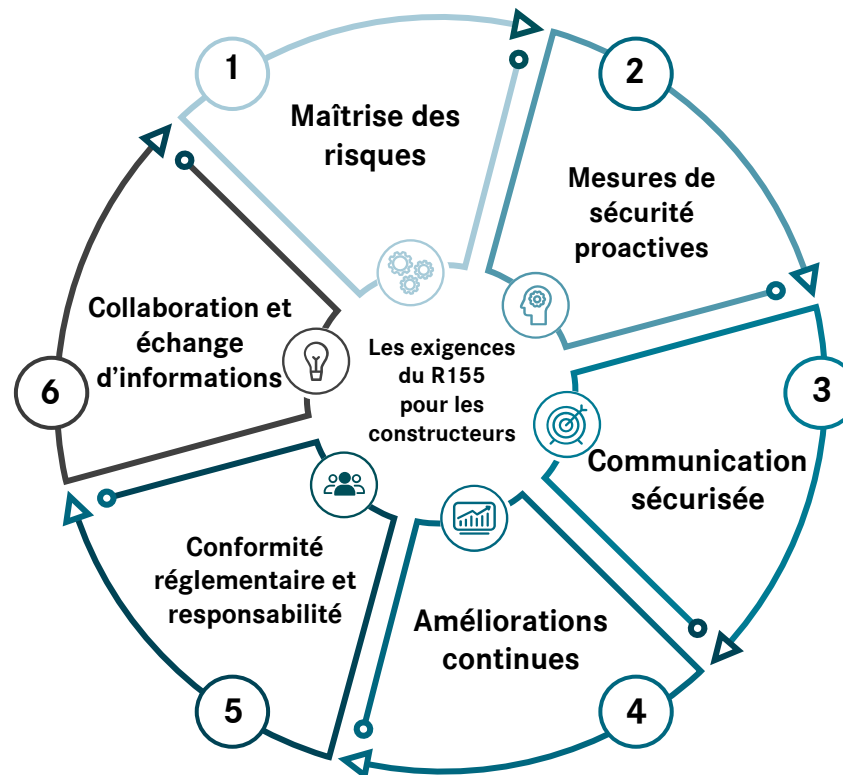
1

Favoriser la collaboration entre les acteurs impliqués pour **partager les meilleures pratiques, les cyber-risques identifiés et les connaissances** pour améliorer la cyber sécurité du véhicule.

6

Conformité aux **exigences légales** et aux normes du secteur, avec une **responsabilité claire** en matière de cybersécurité **au sein de l'organisation**.

5



Mettre en œuvre **des mesures techniques et organisationnelles** solides pour prévenir, détecter et répondre aux cybermenaces.

2

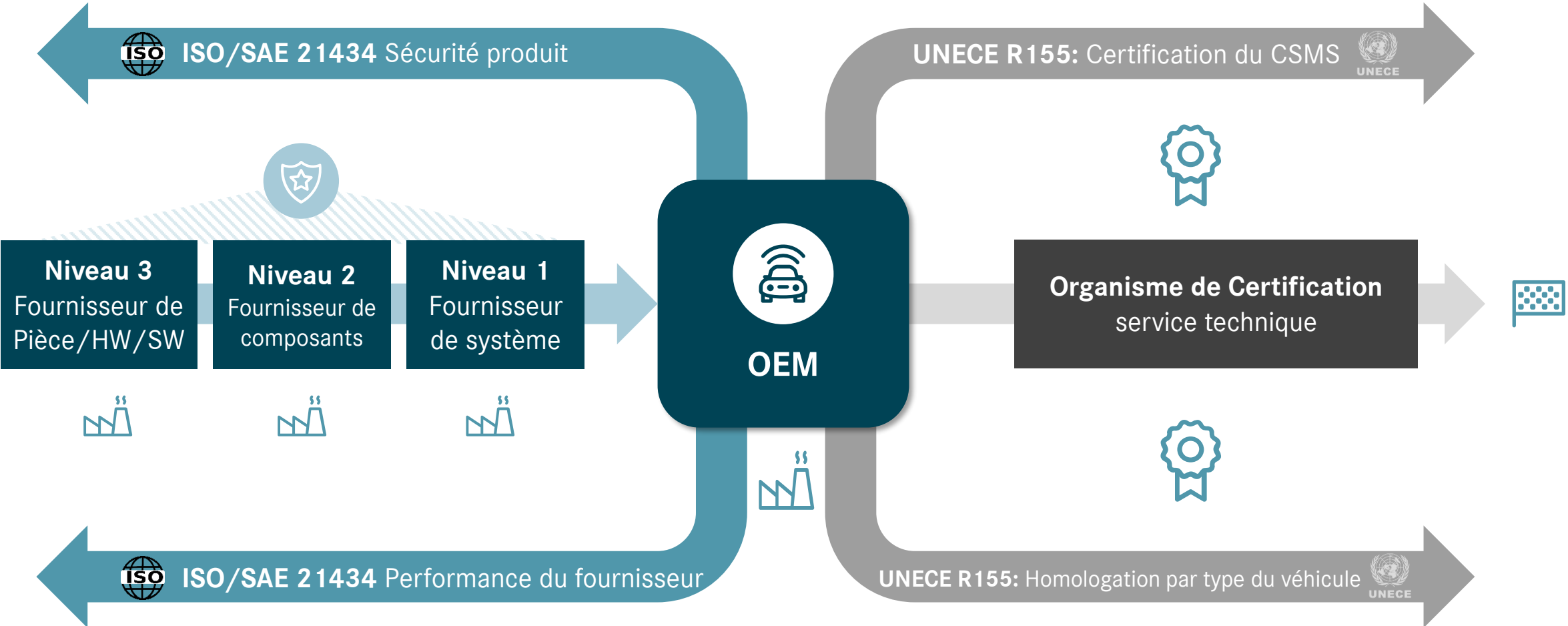
Assurer une communication sécurisée à l'intérieur du véhicule et avec les systèmes externes **pour protéger l'intégrité et la confidentialité des données**.

3

Engagement de surveillance, d'évaluation et d'amélioration continues des mesures de cybersécurité pour répondre aux nouvelles menaces.

4

Quel est le lien entre ISO/SAE 21434 et UNECE R155 ?





Comment se positionne Daimler Buses ?

Quelle est la position de Daimler Buses vis-à-vis du respect du règlement UNECE R155 ?



CSMS §



Certifié depuis mai 2022



Réception par type §

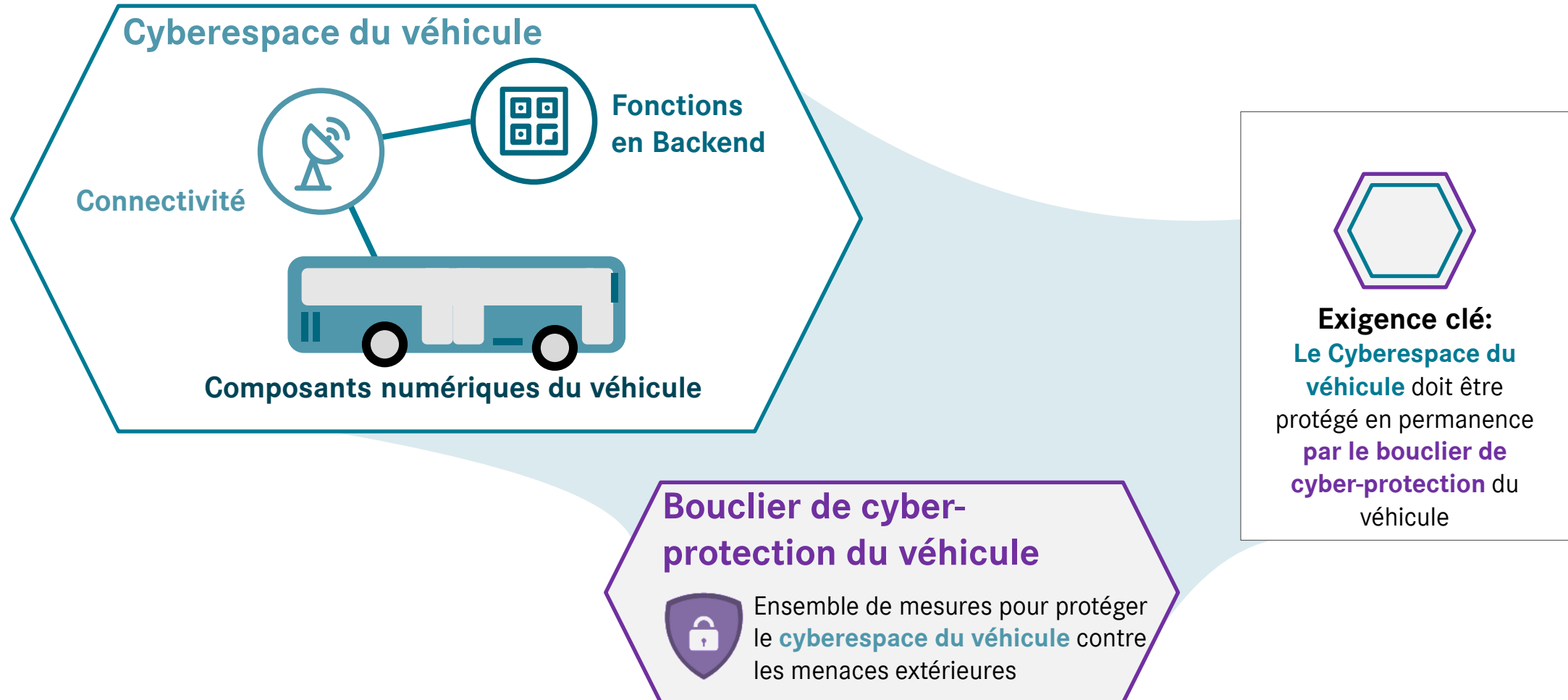


Certification régulière depuis avril 2023



Daimler Buses dispose d'un système **CSMS certifié** qui **garantit que le véhicule** entrant dans le champ d'application du règlement R155 **satisfait aux exigences de l'homologation par type**.

Comment le nouveau contexte réglementaire affecte-t-il la cybersécurité des véhicules ?

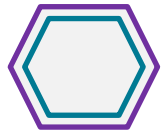


Comment sécuriser le cyberspace des véhicules ?



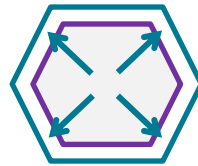
Déclencheur

Mesures à prendre

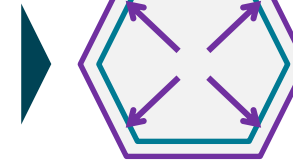


Exigence clé:
Le **Cyberspace du véhicule** doit être protégé en permanence **par le bouclier de cyber-protection** du véhicule

Développement de nouvelles fonctions



L'ajout de fonctionnalités numériques au **cyberspace du véhicule** (par ex. freinage, ADAS) crée de nouvelles vulnérabilités



Véhicule en cours de développement :

Adapter le **bouclier de cyber-protection du véhicule** aux nouvelles fonctionnalités

Véhicule après développement:

Mise à jour du **bouclier de cyber-protection du véhicule** sur les véhicules en production pour permettre de nouvelles fonctionnalités

Détection de nouvelles menaces ou vulnérabilités



Nouvelles vulnérabilités qui compromettent l'efficacité du bouclier de **cyber-protection du véhicule** (par ex. spectre2, meltdown2)



Véhicule en cours de développement :

Mise à jour du **bouclier de cybersécurité du véhicule** pour protéger contre les menaces nouvelles et potentielles.

Véhicule après développement :

- a) Mise à jour du **bouclier de cyber-protection du véhicule** pour les véhicules en production de série
- b) Mise à jour du **bouclier de cyber-protection du véhicule** pour les véhicules en exploitation.

Conclusion:



La cybersécurité du véhicule protège les systèmes du véhicule contre les accès non autorisés, les manipulations ou les dysfonctionnements.



À partir de **juillet 2024**, les constructeurs et les autobus/autocars devront se soumettre aux procédures d'homologation du règlement **UNECE R155**.



Daimler Buses dispose d'un système de gestion de la Cybersécurité (**CSMS**) certifié, qui répond aux exigences du règlement **UNECE R155** pour les véhicules entrant dans le champ d'application.