Numai textele originale CEE-ONU au efect juridic în temeiul dreptului public internațional. Situația și data intrării în vigoare ale prezentului regulament trebuie verificate în cea mai recentă versiune a documentului de situație CEE-ONU TRANS/WP.29/343, disponibil la adresa: https://unece.org/status-1958-agreement-and-annexed-regulations

Regulamentul ONU nr. 155 – Dispoziții uniforme referitoare la omologarea vehiculelor în ceea ce privește securitatea cibernetică și sistemul de gestionare a securității cibernetice [2025/5]

Include toate textele valabile până la:

Suplimentul 3 la versiunea originală a regulamentului – Data intrării în vigoare: 10 ianuarie 2025

Prezentul document este strict un instrument de documentare. Textele autentice și obligatorii din punct de vedere juridic sunt:

— ECE/TRANS/WP.29/2020/79 (astfel cum a fost modificat prin ECE/TRANS/WP.29/2020/94 și ECE/TRANS/WP.29/2020/97)

— ECE/TRANS/WP.29/2022/54

— ECE/TRANS/WP.29/2023/70; și

— ECE/TRANS/WP.29/2024/55

CUPRINS

Regulamentul

1. Domeniu de aplicare
2. Definiții
3. Cerere de omologare
4. Marcaje
5. Omologarea
6. Certificat de conformitate pentru sistemul de gestionare a securității cibernetice
7. Specificații
8. Modificarea tipului de vehicul și extinderea omologării de tip
9. Conformitatea producției
10. Sancțiuni în cazul nerespectării conformității producției
11. Întreruperea definitivă a producției
12. Denumirile și adresele serviciilor tehnice responsabile cu efectuarea încercărilor de omologare, precum și ale autorităților de omologare de tip

Anexe

1. Fișa de informații
2. Comunicare
3. Dispunerea mărcii de omologare
4. Model de certificat de conformitate pentru sistemul de gestionare a securității cibernetice
5. Lista amenințărilor și a măsurilor de atenuare corespunzătoare

1. Domeniu de aplicare

1.1. Prezentul regulament se aplică vehiculelor din categoriile L, M, N și O, în ceea ce privește securitatea cibernetică, dacă sunt echipate cu cel puțin o unitate electronică de control.

1.2. Prezentul regulament nu aduce atingere altor regulamente ONU, legislațiilor regionale sau naționale care reglementează accesul părților autorizate la vehicul, la datele, funcțiile și resursele acestuia, precum și condițiile de acces. De asemenea, acesta nu aduce atingere aplicării legislației naționale și regionale privind confidențialitatea și protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal.

1.3. Prezentul regulament nu aduce atingere altor regulamente ONU, legislației naționale sau regionale care reglementează dezvoltarea și instalarea/integrarea în sistem a pieselor de schimb și a componentelor, fizice și digitale, în ceea ce privește securitatea cibernetică.

2. Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

2.1. „Tip de vehicul” înseamnă vehicule care nu diferă cel puțin în privința următoarelor aspecte esențiale:

(a) desemnarea tipului de vehicul de către producător;

(b) aspecte esențiale ale arhitecturii electrice/electronice și ale interfețelor externe în ceea ce privește securitatea cibernetică.

2.2. „Securitate cibernetică” înseamnă starea în care vehiculele rutiere și funcțiile acestora sunt protejate împotriva amenințărilor cibernetice ce vizează componentele electrice sau electronice.

2.3. „Sistem de gestionare a securității cibernetice (*Cyber Security Management System* – CSMS)” înseamnă o abordare sistematică bazată pe riscuri care definește guvernanța, procesele și responsabilitățile organizaționale pentru tratarea riscului asociat amenințărilor cibernetice ce vizează vehiculele și protejarea acestora împotriva atacurilor cibernetice.

2.4. „Sistem” înseamnă un set de componente și/sau subsisteme care implementează una sau mai multe funcții.

2.5. „Etapa de dezvoltare” înseamnă perioada anterioară omologării de tip a unui tip de vehicul.

2.6. „Etapa de producție” înseamnă durata producției unui tip de vehicul.

2.7. „Etapa de postproducție” înseamnă perioada în care un tip de vehicul nu mai este produs până la sfârșitul ciclului de viață al tuturor vehiculelor de tipul respectiv. Vehiculele care reprezintă un anumit tip de vehicul vor fi operaționale în această etapă, dar nu vor mai fi produse. Etapa se încheie atunci când nu mai există vehicule operaționale de un anumit tip de vehicul.

2.8. „Măsură de atenuare” înseamnă o măsură care reduce riscul.

2.9. „Risc” înseamnă potențialul ca o anumită amenințare să exploateze vulnerabilitățile unui vehicul și, prin urmare, să provoace daune organizației sau unei persoane.

2.10. „Evaluarea riscurilor” înseamnă procesul general de identificare, recunoaștere și descriere a riscurilor (identificarea riscurilor), pentru a înțelege natura riscului și a determina nivelul acestuia (analiza riscurilor), precum și de comparare a rezultatelor analizei riscurilor cu criteriile de risc pentru a stabili dacă riscul și/sau amploarea acestuia sunt acceptabile sau tolerabile (evaluarea riscului).

2.11. „Gestionarea riscurilor” înseamnă o serie de activități coordonate pentru a administra și controla o organizație în ceea ce privește riscul.

2.12. „Amenințare” înseamnă o cauză potențială a unui incident nedorit, care poate afecta negativ un sistem, o organizație sau o persoană fizică.

2.13. „Vulnerabilitatea” înseamnă un punct slab al unui activ sau al unei măsuri de atenuare, care poate fi exploatat de una sau mai multe amenințări.

3. Cerere de omologare

3.1. Cererea de omologare a unui tip de vehicul cu privire la sistemul de securitate cibernetică se înaintează de către producătorul vehiculului sau de către reprezentantul autorizat al acestuia.

3.2. Cererea trebuie să fie însoțită de documentele menționate în continuare, în trei exemplare, precum și de următoarele informații:

3.2.1. O descriere a tipului de vehicul în ceea ce privește elementele menționate în anexa 1 la prezentul regulament.

3.2.2. În cazurile în care aceste informații sunt reglementate de drepturile de proprietate intelectuală sau constituie know-how specific al producătorului sau al furnizorilor săi, producătorul sau furnizorii săi trebuie să furnizeze suficiente informații pentru a permite efectuarea corectă a verificărilor prevăzute de regulament. Aceste informații trebuie tratate în mod confidențial.

3.2.3. Certificat de conformitate pentru CSMS în conformitate cu punctul 6 din prezentul regulament.

3.3. Documentația este pusă la dispoziție în două părți:

(a) dosarul cu documentația oficială pentru omologare, conținând materialul specificat în anexa 1, care trebuie furnizat autorității de omologare sau serviciului tehnic al acesteia la momentul depunerii cererii de omologare de tip. Acest dosar cu documentația trebuie utilizat de autoritatea de omologare sau de serviciul tehnic al acesteia ca referință de bază pentru procesul de omologare. Autoritatea de omologare sau serviciul tehnic al acesteia se asigură că acest dosar cu documentația rămâne disponibil cel puțin 10 ani de la momentul întreruperii definitive a producției tipului de vehicul în cauză;

(b) materialele suplimentare relevante pentru cerințele prezentului regulament pot fi păstrate de producător, dar sunt puse la dispoziție pentru inspecție la momentul omologării de tip. Producătorul se asigură că orice material pus la dispoziție pentru inspecție la momentul omologării de tip rămâne disponibil pe o perioadă de cel puțin 10 ani de la momentul încetării definitive a producției tipului de vehicul în cauză.

4. Marcaj

4.1. Pe fiecare vehicul conform cu un tip de vehicul omologat în temeiul prezentului regulament trebuie aplicată, în mod vizibil și într-un loc ușor accesibil, menționat în fișa de omologare, o marcă de omologare internațională care include următoarele elemente:

4.1.1. un cerc în interiorul căruia se află litera „E” urmată de numărul distinctiv al țării care a acordat omologarea;

4.1.2. numărul prezentului regulament, urmat de litera „R”, o liniuță și numărul de omologare, în dreapta cercului menționat la punctul 4.1.1 de mai sus.

4.2. În cazul în care vehiculul corespunde unui tip de vehicul omologat în temeiul unuia sau mai multor regulamente anexate la acord, în țara care a acordat omologarea în temeiul prezentului regulament, simbolul prevăzut la punctul 4.1.1 de mai sus nu trebuie repetat; în această situație, numărul regulamentului și numerele de omologare, precum și simbolurile suplimentare ale tuturor regulamentelor în temeiul cărora s-a acordat omologarea în țara care a acordat omologarea în conformitate cu prezentul regulament se introduc în coloane verticale la dreapta simbolului prevăzut la punctul 4.1.1.

4.3. Marca de omologare trebuie să fie ușor lizibilă și de neșters.

4.4. Marca de omologare trebuie să fie amplasată alături de plăcuța cu date a vehiculului aplicată de producător sau pe aceasta.

4.5. În anexa 3 la prezentul regulament sunt prezentate exemple de dispunere a mărcilor de omologare.

5. Omologarea

5.1. Autoritățile de omologare acordă, după caz, omologarea de tip în ceea ce privește securitatea cibernetică, numai tipurilor de vehicule care îndeplinesc cerințele prezentului regulament.

5.1.1. Autoritatea de omologare sau serviciul tehnic verifică prin controale ale documentelor dacă producătorul vehiculului a luat măsurile necesare relevante pentru tipul de vehicul pentru:

(a) a colecta și verifica informațiile solicitate în temeiul prezentului regulament prin intermediul lanțului de aprovizionare, astfel încât să demonstreze că riscurile legate de furnizori sunt identificate și gestionate;

(b) a documenta evaluarea riscurilor (efectuată în timpul etapei de dezvoltare sau retroactiv), rezultatele încercărilor și măsurile de atenuare aplicate tipului de vehicul, inclusiv informații de proiectare care sprijină evaluarea riscurilor;

(c) a pune în aplicare măsuri de securitate cibernetică adecvate în proiectarea tipului de vehicul;

(d) a detecta și a răspunde la posibile atacuri de securitate cibernetică;

(e) a înregistra date pentru a sprijini detectarea atacurilor cibernetice și a furniza capacitatea de analiză criminalistică a datelor necesară pentru a permite analiza tentativelor sau a atacurilor cibernetice reușite.

5.1.2. Autoritatea de omologare sau serviciul tehnic verifică prin încercarea unui vehicul de tipul vehiculului în cauză dacă producătorul acestuia a pus în aplicare măsurile de securitate cibernetică pe care le-a documentat. Încercările sunt efectuate de către autoritatea de omologare sau de serviciul tehnic însuși sau în colaborare cu producătorul vehiculului prin eșantionare. Eșantionarea se concentrează asupra riscurilor care sunt evaluate ca fiind ridicate în timpul evaluării riscurilor, însă fără a se limita la acestea.

5.1.3. Autoritatea de omologare sau serviciul tehnic refuză acordarea omologării de tip în ceea ce privește securitatea cibernetică dacă producătorul vehiculului nu a îndeplinit una sau mai multe dintre cerințele menționate la punctul 7.3, în special dacă:

(a) producătorul vehiculului nu a efectuat evaluarea exhaustivă a riscurilor menționată la punctul 7.3.3, inclusiv în cazul în care producătorul nu a ținut cont de toate riscurile legate de amenințările menționate în partea A din anexa 5;

(b) producătorul vehiculului nu a protejat tipul de vehicul împotriva riscurilor identificate în cadrul evaluării riscurilor efectuate de producătorul vehiculului sau nu au fost puse în aplicare măsuri de atenuare proporționale, conform cerințelor de la punctul 7;

(c) producătorul vehiculului nu a pus în aplicare măsuri adecvate și proporționale pentru a securiza mediile dedicate de pe tipul de vehicul în cauză (dacă sunt prevăzute) pentru stocarea și executarea software-ului, a serviciilor, a aplicațiilor sau a datelor după introducerea pe piață;

(d) producătorul vehiculului nu a efectuat, înainte de omologare, încercări adecvate și suficiente pentru a verifica eficacitatea măsurilor de securitate adoptate.

5.1.4. Autoritatea de omologare care efectuează evaluarea refuză, de asemenea, să acorde omologarea de tip în ceea ce privește securitatea cibernetică în cazul în care autoritatea de omologare sau serviciul tehnic nu a primit suficiente informații de la producătorul vehiculului pentru a evalua securitatea cibernetică a tipului de vehicul.

5.2. Anunțul privind omologarea, extinderea sau refuzul omologării unui tip de vehicul în temeiul prezentului regulament se comunică părților la Acordul din 1958 care aplică prezentul regulament prin intermediul unui formular conform cu modelul prevăzut în anexa 2 la prezentul regulament.

5.3. Autoritățile de omologare nu acordă nicio omologare de tip fără a verifica dacă producătorul a pus în aplicare mecanisme și proceduri satisfăcătoare pentru a gestiona în mod adecvat aspectele de securitate cibernetică care fac obiectul prezentului regulament.

5.3.1. Autoritatea de omologare și serviciile sale tehnice se asigură, pe lângă criteriile stabilite în anexa 2 la Acordul din 1958, că dețin:

(a) personal competent cu abilități adecvate în materie de securitate cibernetică și cunoștințe specifice privind evaluarea riscurilor pentru automobile ([1]);

(b) proceduri instituite pentru evaluarea uniformă în conformitate cu prezentul regulament.

5.3.2. Fiecare parte contractantă care aplică prezentul regulament notifică și informează prin intermediul autorității sale de omologare alte autorități de omologare ale părților contractante care aplică prezentul regulament ONU cu privire la metoda și criteriile considerate ca bază de către autoritatea de notificare pentru a evalua caracterul adecvat al măsurilor luate în conformitate cu prezentul regulament și, în special, cu punctele 5.1, 7.2 și 7.3.

Aceste informații trebuie distribuite: (a) numai înainte de acordarea unei omologări în conformitate cu prezentul regulament pentru prima dată; și (b) de fiecare dată când metoda sau criteriile de evaluare sunt actualizate.

Aceste informații sunt menite a fi distribuite în scopul colectării și analizei celor mai bune practici și în vederea asigurării aplicării convergente a prezentului regulament de către toate autoritățile de omologare care aplică prezentul regulament.

5.3.3. Informațiile menționate la punctul 5.3.2 se încarcă, în limba engleză, în baza de date online securizată „DETA” ([2]), instituită de Comisia Economică pentru Europa a Organizației Națiunilor Unite, în timp util și cu cel puțin 14 zile înainte de acordarea omologării pentru prima dată în conformitate cu metodele și criteriile de evaluare în cauză. Informațiile trebuie să fie suficiente pentru a se putea înțelege nivelurile minime de performanță care au fost adoptate de autoritatea de omologare pentru fiecare cerință specifică menționată la punctul 5.3.2, precum și procesele și măsurile pe care autoritatea le aplică pentru a verifica dacă aceste niveluri minime de performanță sunt îndeplinite ([3]).

5.3.4. Autoritățile de omologare care primesc informațiile menționate la punctul 5.3.2 pot transmite observații autorității de omologare notificatoare prin încărcarea lor în DETA în termen de 14 zile de la data notificării.

5.3.5. Dacă nu este posibil ca autoritatea care acordă omologarea să țină seama de observațiile primite în conformitate cu punctul 5.3.4, autoritățile de omologare care au transmis observații și autoritatea care acordă omologarea vor încerca să obțină clarificări suplimentare în conformitate cu anexa 6 la Acordul din 1958. Grupul de lucru subsidiar relevant ([4]) al Forumului mondial pentru armonizarea regulamentelor privind vehiculele (WP.29) pentru prezentul regulament convine asupra unei interpretări comune a metodelor și criteriilor de evaluare. ([5]) Această interpretare comună trebuie pusă în aplicare, iar toate autoritățile de omologare trebuie să elibereze omologări de tip în conformitate cu prezentul regulament.

([1]) De exemplu, ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.
([2]) https://www.unece.org/trans/main/wp29/datasharing.html.
([3]) Îndrumările privind informațiile detaliate (de exemplu, metoda, criteriile, nivelul de performanță) care trebuie încărcate și formatul acestora trebuie să fie furnizate în documentul de interpretare care este în curs de pregătire de către Grupul operativ privind securitatea cibernetică și alte probleme legate de transmisiunile wireless pentru cea de a 7-a sesiune a GRVA.
([4]) Grupul de lucru privind vehiculele automatizate/autonome și conectate (GRVA).
([5]) Această interpretare trebuie reflectată în documentul de interpretare menționat în nota de subsol de la punctul 5.3.3.

5.3.6. Fiecare autoritate de omologare care acordă o omologare de tip în conformitate cu prezentul regulament notifică alte autorități de omologare cu privire la omologarea acordată. Omologarea de tip împreună cu documentația suplimentară se încarcă în DETA, în limba engleză, de către autoritatea de omologare în termen de 14 zile de la data acordării omologării. ([6])

5.3.7. Părțile contractante pot studia omologările acordate pe baza informațiilor încărcate în conformitate cu punctul 5.3.6. În cazul oricăror opinii divergente între părțile contractante, acestea se vor soluționa în conformitate cu articolul 10 și cu anexa 6 la Acordul din 1958. De asemenea, părțile contractante vor informa Grupul de lucru subsidiar relevant al Forumului mondial pentru armonizarea regulamentelor privind vehiculele (WP.29) cu privire la interpretările divergente în sensul anexei 6 la Acordul din 1958. Grupul de lucru relevant va sprijini soluționarea opiniilor divergente și se poate consulta cu WP.29 în acest sens, dacă este necesar.

5.4. În sensul punctului 7.2 din prezentul regulament, producătorul se asigură că aspectele de securitate cibernetică acoperite de prezentul regulament sunt puse în aplicare.

6. Certificat de conformitate pentru sistemul de gestionare a securității cibernetice

6.1. Părțile contractante desemnează o autoritate de omologare pentru a efectua evaluarea producătorului și pentru a emite un certificat de conformitate pentru CSMS.

6.2. Producătorul vehiculului sau reprezentantul acestuia acreditat în mod corespunzător trebuie să depună o cerere de eliberare a unui certificat de conformitate pentru sistemul de gestionare a securității cibernetice.

6.3. Aceasta trebuie să fie însoțită de documentele menționate în continuare, în trei exemplare, și de următoarele informații:

6.3.1. documentele care descriu sistemul de gestionare a securității cibernetice;

6.3.2. o declarație semnată, utilizând modelul definit în apendicele 1 la anexa 1.

6.4. În contextul evaluării, producătorul declară, folosind modelul definit în apendicele 1 la anexa 1, și demonstrează în mod satisfăcător pentru autoritatea de omologare sau serviciul tehnic al acesteia că deține procesele necesare pentru a îndeplini toate cerințele de securitate cibernetică în conformitate cu prezentul regulament.

6.5. La finalizarea în mod satisfăcător a evaluării și la primirea unei declarații semnate de către producător în conformitate cu modelul definit în apendicele 1 la anexa 1, producătorului trebuie să i se elibereze un certificat denumit Certificat de conformitate pentru CSMS, astfel cum este descris în anexa 4 la prezentul regulament (denumit în continuare „Certificat de conformitate pentru CSMS”).

6.6. Autoritatea de omologare sau serviciul tehnic al acesteia utilizează modelul prezentat în anexa 4 la prezentul regulament pentru Certificatul de conformitate pentru CSMS.

6.7. Certificatul de conformitate pentru CSMS are o valabilitate de cel mult trei ani de la data eliberării, cu excepția cazului în care este retras.

6.8. Autoritatea de omologare care a acordat certificatul de conformitate pentru CSMS poate verifica în orice moment dacă cerințele pentru acordarea acestuia sunt îndeplinite în continuare. Autoritatea de omologare trebuie să retragă certificatul de conformitate pentru CSMS în cazul în care cerințele prevăzute în prezentul regulament nu mai sunt îndeplinite.

([6]) Informații suplimentare cu privire la cerințele minime pentru dosarul cu documentația vor fi elaborate de GRVA în cursul celei de a șaptea sesiuni.

6.9. Producătorul informează autoritatea de omologare sau serviciul tehnic al acesteia cu privire la orice modificare care va afecta relevanța certificatului de conformitate pentru CSMS. După consultarea producătorului, autoritatea de omologare sau serviciul tehnic al acesteia decide dacă sunt necesare noi verificări.

6.10. Producătorul va solicita un nou certificat de conformitate pentru CSMS sau prelungirea celui existent, în timp util, permițând autorității de omologare să își finalizeze evaluarea înainte de sfârșitul perioadei de valabilitate a certificatului de conformitate pentru CSMS. Autoritatea de omologare eliberează, sub rezerva unei evaluări pozitive, un nou certificat de conformitate pentru CSMS sau prelungește valabilitatea acestuia cu o perioadă suplimentară de trei ani. Autoritatea de omologare verifică dacă CSMS respectă în continuare cerințele prezentului regulament. Autoritatea de omologare eliberează un nou certificat în cazurile în care modificările au fost aduse la cunoștința sa sau a serviciului tehnic al acesteia, iar modificările au fost reevaluate pozitiv.

6.11. Expirarea sau retragerea certificatului de conformitate al producătorului pentru CSMS trebuie considerată, în ceea ce privește tipurile de vehicule pentru care CSMS în cauză a fost relevant, ca o modificare a omologării, astfel cum se menționează la punctul 8, putând include retragerea omologării, dacă nu mai sunt îndeplinite condițiile pentru acordarea omologării.

7. Specificații

7.1. Specificații generale

7.1.1. Cerințele prezentului regulament nu restricționează dispozițiile sau cerințele altor regulamente ONU.

7.2. Cerințe pentru sistemul de gestionare a securității cibernetice

7.2.1. În vederea efectuării evaluării, autoritatea de omologare sau serviciul tehnic al acesteia verifică dacă producătorul vehiculului deține un sistem de gestionare a securității cibernetice și conformitatea acestuia cu prezentul regulament.

7.2.2. Sistemul de gestionare a securității cibernetice acoperă următoarele aspecte:

7.2.2.1. Producătorul vehiculului demonstrează autorității de omologare sau serviciului tehnic al acesteia că sistemul său de gestionare a securității cibernetice se aplică următoarelor etape:

(a) etapa de dezvoltare;

(b) etapa de producție;

(c) etapa de postproducție.

7.2.2.2. Producătorul vehiculului trebuie să demonstreze că procesele utilizate în cadrul sistemului său de gestionare a securității cibernetice asigură luarea adecvată în considerare a aspectelor de securitate, inclusiv a riscurilor și a măsurilor de atenuare enumerate în anexa 5. Acestea includ:

(a) procesele utilizate în cadrul organizației producătorului pentru gestionarea securității cibernetice;

(b) procesele utilizate pentru identificarea riscurilor care vizează tipurile de vehicule. În cadrul acestor procese, trebuie luate în considerare amenințările descrise în partea A din anexa 5 și alte amenințări relevante;

(c) procesele utilizate pentru evaluarea, clasificarea și tratarea riscurilor identificate;

(d) procesele instituite pentru a verifica dacă riscurile identificate sunt gestionate în mod corespunzător;

(e) procesele utilizate pentru testarea securității cibernetice a unui tip de vehicul;

(f) procesele utilizate pentru asigurarea caracterului actual al evaluării riscurilor;

(g) procesele utilizate pentru a monitoriza, a detecta și a răspunde la atacurile cibernetice, amenințările cibernetice și vulnerabilități în funcție de tipurile de vehicule și procesele utilizate pentru a evalua dacă măsurile de securitate cibernetică puse în aplicare sunt încă eficace din perspectiva noilor amenințări cibernetice și a noilor vulnerabilități care au fost identificate;

(h) procesele utilizate pentru furnizarea de date relevante în sprijinul analizei tentativelor sau a atacurilor cibernetice reușite.

7.2.2.3. Producătorul vehiculului trebuie să demonstreze că procesele utilizate în cadrul sistemului său de gestionare a securității cibernetice vor asigura, pe baza clasificării menționate la punctul 7.2.2.2 literele (c) și (g), atenuarea amenințărilor cibernetice și a vulnerabilităților care necesită un răspuns din partea producătorului vehiculului într-un termen rezonabil.

7.2.2.4. Producătorul vehiculului trebuie să demonstreze că procesele utilizate în cadrul sistemului său de gestionare a securității cibernetice vor asigura continuitatea monitorizării menționate la punctul 7.2.2.2 litera (g). Aceasta:

(a) include în cadrul monitorizării vehiculele după prima înmatriculare;

(b) include capacitatea de a analiza și a detecta amenințările cibernetice, vulnerabilitățile și atacurile cibernetice pe baza datelor și jurnalelor vehiculelor. Această capacitate trebuie să respecte punctul 1.3 și drepturile de confidențialitate ale proprietarilor de mașini sau ale conducătorilor auto, în special cu privire la consimțământ.

7.2.2.5. Producătorul vehiculului trebuie să demonstreze modul în care sistemul său de gestionare a securității cibernetice va gestiona dependențele care ar putea exista în raport cu furnizorii contractați, furnizorii de servicii sau suborganizațiile producătorului în ceea ce privește cerințele de la punctul 7.2.2.2.

7.3. Cerințe privind tipurile de vehicule

7.3.1. Producătorul trebuie să dețină un certificat de conformitate valabil pentru sistemul de gestionare a securității cibernetice, relevant pentru tipul de vehicul omologat. Cu toate acestea, pentru omologări de tip ale vehiculelor din categoriile M, N și O eliberate înainte de 1 iulie 2024, precum și pentru omologări de tip ale vehiculelor din categoria L eliberate pentru prima dată înainte de 1 iulie 2029, precum și pentru orice extindere a acestora, dacă producătorul vehiculului poate demonstra că tipul de vehicul nu a putut fi dezvoltat în conformitate cu CSMS, atunci acesta trebuie să demonstreze că s-a ținut cont în mod adecvat de aspectele de securitate cibernetică în timpul etapei de dezvoltare a tipului de vehicul în cauză.

7.3.2. Producătorul vehiculului identifică și gestionează, pentru tipul de vehicul omologat, riscurile legate de furnizor.

7.3.3. Producătorul vehiculului identifică elementele critice ale tipului de vehicul și efectuează o evaluare exhaustivă a riscurilor pentru tipul de vehicul în cauză și tratează/gestionează în mod adecvat riscurile identificate. Evaluarea riscurilor ia în considerare elementele individuale ale tipului de vehicul și interacțiunile acestora. Evaluarea riscurilor ia în considerare și interacțiunile cu orice sistem extern. În timpul evaluării riscurilor, producătorul vehiculului ia în considerare riscurile legate de toate amenințările menționate în partea A din anexa 5, precum și orice alt risc relevant.

7.3.4. Producătorul vehiculului protejează tipul de vehicul împotriva riscurilor identificate în cadrul evaluării riscurilor efectuate de producătorul vehiculului. Pentru a proteja tipul de vehicul, trebuie adoptate măsuri de atenuare proporționale. Măsurile de atenuare puse în aplicare includ toate măsurile menționate în părțile B și C din anexa 5 relevante pentru riscurile identificate. Cu toate acestea, dacă o măsură de atenuare menționată în partea B sau C din anexa 5 nu este relevantă sau nu este suficientă pentru riscul identificat, producătorul vehiculului se asigură că este pusă în aplicare o altă măsură de atenuare adecvată.

În special, pentru omologări de tip ale vehiculelor din categoriile M, N și O acordate pentru prima oară înainte de 1 iulie 2024 și pentru omologări de tip ale vehiculelor din categoria L acordate pentru prima oară înainte de 1 iulie 2029, precum și pentru fiecare extindere a acestora, producătorul de vehicule se asigură că o altă măsură de atenuare corespunzătoare este pusă în aplicare dacă o măsură de atenuare menționată în partea B sau în partea C din anexa 5 nu este fezabilă din punct de vedere tehnic. Evaluarea respectivă a fezabilității tehnice este furnizată de producător autorității de omologare.

7.3.5. Producătorul vehiculului pune în aplicare măsuri adecvate și proporționale pentru a securiza mediile dedicate de pe tipul de vehicul în cauză (dacă sunt prevăzute) pentru stocarea și executarea software-ului, a serviciilor, a aplicațiilor sau a datelor după introducerea pe piață.

7.3.6. Producătorul vehiculului efectuează, înainte de omologarea de tip, încercări adecvate și suficiente pentru a verifica eficacitatea măsurilor de securitate puse în aplicare.

7.3.7. Producătorul vehiculului pune în aplicare măsuri în legătură cu tipul de vehicul pentru:

(a) a detecta și preveni atacurile cibernetice împotriva vehiculelor care fac parte din tipul de vehicul în cauză;

(b) a sprijini capacitatea de monitorizare a producătorului vehiculului în ceea ce privește detectarea amenințărilor, a vulnerabilităților și a atacurilor cibernetice relevante pentru tipul vehiculului;

(c) a asigura capacitatea de analiză criminalistică a datelor pentru a permite analiza tentativelor sau a atacurilor cibernetice reușite.

7.3.8. Modulele criptografice utilizate în sensul prezentului regulament trebuie să respecte standarde consensuale. Dacă acestea nu respectă standardele consensuale, atunci producătorul vehiculului trebuie să justifice utilizarea lor.

7.4. Dispoziții privind raportarea

7.4.1. Producătorul vehiculului raportează cel puțin o dată pe an (sau mai frecvent dacă este relevant) autorității de omologare sau serviciului tehnic al acesteia rezultatul activităților sale de monitorizare, astfel cum sunt definite la punctul 7.2.2.2 litera (g); această raportare trebuie să includă informații relevante privind noile atacuri cibernetice. De asemenea, producătorul vehiculului raportează și confirmă autorității de omologare sau serviciului tehnic al acesteia că măsurile de atenuare privind securitatea cibernetică adoptate pentru tipurile sale de vehicule sunt încă eficace și că au fost întreprinse acțiunile suplimentare necesare.

7.4.2. Autoritatea de omologare sau serviciul tehnic verifică informațiile furnizate și, dacă este necesar, solicită producătorului vehiculului să remedieze orice ineficiență detectată.

În cazul în care raportarea sau răspunsul nu este suficient(ă), autoritatea de omologare poate decide retragerea CSMS în conformitate cu punctul 6.8.

8. Modificarea tipului de vehicul și extinderea omologării de tip

8.1. Orice modificare a tipului de vehicul care afectează performanța sa tehnică în ceea ce privește securitatea cibernetică și/sau documentația solicitată în prezentul regulament este notificată autorității de omologare care a omologat tipul de vehicul. După notificare, autoritatea de omologare poate:

8.1.1. considera că modificările aduse respectă în continuare cerințele și documentația omologării de tip existente; sau

8.1.2. poate trece la evaluarea complementară necesară în conformitate cu punctul 5 și solicita, după caz, un raport suplimentar de încercare de la serviciul tehnic responsabil cu efectuarea încercărilor.

8.1.3. Confirmarea, extinderea sau refuzul omologării, specificând modificările, se comunică prin intermediul unei fișe de comunicare conforme cu modelul prezentat în anexa 2 la prezentul regulament. Autoritatea de omologare care acordă o extindere a omologării atribuie un număr de serie acestei extinderi și informează celelalte părți la Acordul din 1958 care aplică prezentul regulament cu privire la acest fapt prin intermediul unei fișe de comunicare conforme cu modelul prezentat în anexa 2 la prezentul regulament.

9. Conformitatea producției

9.1. Procedurile privind conformitatea producției sunt conforme cu cele stabilite în anexa 1 la Acordul din 1958 (E/ECE/TRANS/505/Rev.3), ținând seama de următoarele cerințe:

9.1.1. titularul omologării trebuie să asigure că rezultatele încercărilor de conformitate a producției sunt înregistrate și că documentele anexate rămân disponibile pentru o perioadă stabilită împreună cu autoritatea de omologare sau cu serviciul tehnic al acesteia. Această perioadă nu trebuie să depășească 10 ani de la data încetării definitive a producției;

9.1.2. autoritatea de omologare care a acordat omologarea de tip poate verifica în orice moment metodele de control al conformității aplicate în fiecare unitate de producție. Frecvența normală a acestor verificări este de o dată la trei ani.

10. Sancțiuni în cazul nerespectării conformității producției

10.1. Omologarea de tip acordată pentru un tip de vehicul în temeiul prezentului regulament poate fi retrasă în cazul în care nu se respectă cerințele prevăzute în prezentul regulament sau în cazul în care vehiculele din eșantion nu respectă cerințele prevăzute în prezentul regulament.

10.2. În cazul în care o autoritate de omologare retrage o omologare pe care a acordat-o anterior, aceasta trebuie să informeze de îndată celelalte părți contractante care aplică prezentul regulament, printr-o fișă de comunicare conformă cu modelul din anexa 2 la prezentul regulament.

11. Întreruperea definitivă a producției

11.1. În cazul în care titularul omologării încetează definitiv să producă un tip de vehicul omologat în conformitate cu prezentul regulament, acesta informează autoritatea care a acordat omologarea cu privire la aceasta. La primirea comunicării corespunzătoare, autoritatea respectivă informează în acest sens celelalte părți contractante la acord care aplică prezentul regulament, prin intermediul unei copii a formularului de omologare care conține la final mențiunea semnată și datată „PRODUCȚIE OPRITĂ” redactată cu majuscule.

12. Denumirile și adresele serviciilor tehnice responsabile cu efectuarea încercărilor de omologare, precum și ale autorităților de omologare de tip

12.1. Părțile contractante la acord care aplică prezentul regulament comunică Secretariatului Organizației Națiunilor Unite denumirile și adresele serviciilor tehnice responsabile cu efectuarea încercărilor de omologare și ale autorităților de omologare de tip care acordă omologarea și la care trebuie trimise formularele care certifică omologarea, extinderea, refuzul sau retragerea omologării, emise în alte țări.

ANEXA 1

Fișa de informații

Următoarele informații trebuie furnizate, după caz, în trei exemplare și trebuie să fie însoțite de o listă a elementelor incluse. Toate desenele trebuie furnizate la scară adecvată și suficient de detaliat, în format A4 sau pliate în format A4. Fotografiile, dacă există, trebuie să fie suficient de detaliate.

1. Marca (denumirea comercială a producătorului):.....

2. Tipul și descrierea (descrierile) comercială (comerciale) generală (generale):.....

3. Mijloace de identificare a tipului, dacă sunt prezente pe vehicul: .....

4. Amplasamentul marcajului respectiv: .....

5. Categoria (categoriile) vehiculului:.....

6. Numele și adresa producătorului/reprezentantului producătorului: .....

7. Numele și adresa (adresele) fabricii (fabricilor) de asamblare:.....

8. Fotografie (fotografii) și/sau desen(e) ale unui vehicul reprezentativ: .....

9. Securitatea cibernetică

9.1. Caracteristici generale de construcție ale tipului de vehicul, inclusiv privind:

(a) sistemele vehiculelor care sunt relevante pentru securitatea cibernetică a tipului de vehicul;

(b) componentele sistemelor care sunt relevante pentru securitatea cibernetică;

(c) interacțiunile acestor sisteme cu alte sisteme din cadrul tipului de vehicul și cu interfețele externe.

9.2. Reprezentare schematică a tipului de vehicul

9.3. Numărul certificatului de conformitate pentru CSMS:.....

9.4. Documente pentru tipul de vehicul care urmează să fie omologat, care descriu rezultatul evaluării riscurilor și riscurile identificate: .....

9.5. Documente pentru tipul de vehicul care urmează să fie omologat care descriu măsurile de atenuare puse în aplicare cu privire la sistemele enumerate sau pentru tipul de vehicul și modul în care acestea abordează riscurile declarate: .....

9.6. Documente pentru tipul de vehicul care urmează să fie omologat, care descriu protecția mediilor dedicate pentru software, servicii, aplicații sau date după introducerea pe piață:.....

9.7. Documente pentru tipul de vehicul care urmează să fie omologat care descriu încercările utilizate pentru a verifica securitatea cibernetică a tipului de vehicul și a sistemelor sale și rezultatul acestor încercări: .....

9.8. Descrierea modului în care s-a ținut cont de întregul lanț de aprovizionare în ceea ce privește securitatea cibernetică: .....

Apendicele 1

Model de declarație de conformitate a producătorului pentru CSMS

Declarația producătorului privind conformitatea cu cerințele pentru sistemul de gestionare a securității cibernetice

Numele producătorului: .....

Adresa producătorului: .....

..... (Numele producătorului)

atestă că procesele necesare pentru a se conforma cerințelor pentru sistemul de gestionare a securității cibernetice prevăzute la punctul 7.2 din Regulamentul ONU nr. 155 sunt instalate și vor fi menținute.

Redactat la: .....(locul)

Data:.....

Numele semnatarului: .....

Funcția semnatarului:.....

(Ștampila și semnătura reprezentantului producătorului)

ANEXA 2

Comunicare

[format maxim: A4 (210 × 297 mm)]



eliberată de: Denumirea serviciului administrativ:
……
……
……

privind: (2) Acordarea omologării
Omologarea extinsă
Retragerea omologării începând cu zz/ll/aaaa
Refuzul omologării
Întreruperea definitivă a producției

unui tip de vehicul în conformitate cu Regulamentul ONU nr. 155

Nr. omologării: ……

Nr. extinderii: ……

Motivul extinderii: ……

1. Marca (denumirea comercială a producătorului): ……

2. Tipul și descrierea (descrierile) comercială (comerciale) generală (generale) ……

3. Mijloace de identificare a tipului, dacă sunt prezente pe vehicul: ……

3.1. Amplasamentul marcajului respectiv: ……

4. Categoria (categoriile) vehiculului: ……

5. Numele și adresa producătorului/reprezentantului producătorului: ……

6. Numele și adresa (adresele) unității (unităților) de producție. ……

7. Numărul certificatului de conformitate pentru sistemul de gestionare a securității cibernetice ……

8. Serviciul tehnic responsabil cu efectuarea încercărilor: ……

9. Data raportului de încercare: ……

10. Numărul raportului de încercare: ……

11. Observații: (dacă există) ……

12. Locul: ……

(1) Numărul distinctiv al țării care a acordat/extins/refuzat/retras omologarea (a se vedea dispozițiile regulamentului referitoare la omologare).
(2) A se tăia mențiunea necorespunzătoare.

13. Data:……

14. Semnătura: ……

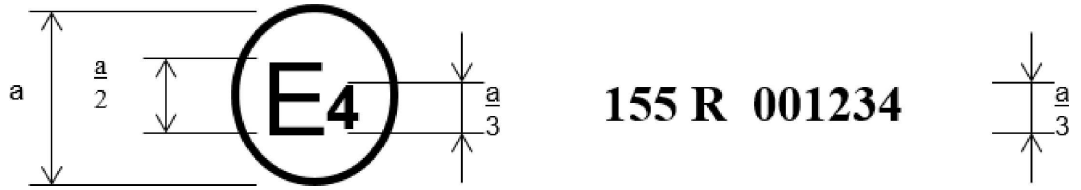
15. Se anexează indexul pachetului de documente depus la autoritatea de omologare, care poate fi obținut la cerere:

ANEXA 3

Dispunerea mărcii de omologare

MODELUL A

(A se vedea punctul 4.2 din prezentul regulament)



a = min. 8 mm

Marca de omologare de mai sus aplicată pe un vehicul indică faptul că tipul de vehicul rutier în cauză a fost omologat în Țările de Jos (E4), în temeiul Regulamentului nr. 155 și sub numărul de omologare 001234. Primele două cifre indică faptul că omologarea a fost acordată în conformitate cu cerințele prezentului regulament, în forma sa originală (00).

ANEXA 4

MODEL DE CERTIFICAT DE CONFORMITATE PENTRU SISTEMUL DE GESTIONARE A SECURITĂȚII CIBERNETICE

Certificat de conformitate pentru sistemul de gestionare a securității cibernetice

cu Regulamentul ONU nr. 155

Numărul certificatului [*Număr de referință*]

[……. *autoritatea de omologare*]

Certifică prin prezenta faptul că

Producătorul: ……

Adresa producătorului: ……

respectă prevederile punctului 7.2 din Regulamentul nr. 155.

Au fost efectuate verificări la: ……

de către (numele și adresa autorității de omologare sau ale serviciului tehnic): ……

Numărul raportului: ……

Certificatul este valabil până la […… *data*]

Adoptat la […… *locul*]

la […… *data*]

[…… *semnătura*]

Documente anexate: descrierea sistemului de gestionare a securității cibernetice de către producător.

ANEXA 5

Lista amenințărilor și a măsurilor de atenuare corespunzătoare

1. Prezenta anexă cuprinde trei părți. Partea A a acestei anexe descrie punctele de referință pentru amenințări, vulnerabilități și metode de atac. Partea B a acestei anexe descrie măsurile de atenuare a amenințărilor care vizează tipurile de vehicule. Partea C descrie măsurile de atenuare a amenințărilor care vizează zonele din afara vehiculelor, de exemplu infrastructura TI bazată pe servere back-end.

2. Părțile A, B și C sunt luate în considerare pentru evaluarea riscurilor și pentru măsurile de atenuare care trebuie puse în aplicare de către producătorii de vehicule.

3. Vulnerabilitatea de nivel înalt și exemplele corespunzătoare au fost indexate în partea A. Aceeași indexare a fost menționată în tabelele din părțile B și C pentru a asocia fiecare atac/vulnerabilitate cu o listă de măsuri de atenuare corespunzătoare.

4. Analiza amenințărilor trebuie să ia în considerare și posibilele efecte ale atacului. Acestea pot ajuta la constatarea gravității unui risc și la identificarea riscurilor suplimentare. Posibilele efecte ale atacului pot include:

   (a) funcționare în siguranță a vehiculului afectată;

   (b) funcții ale vehiculului oprite;

   (c) software modificat, performanță afectată;

   (d) software modificat, fără efecte operaționale;

   (e) încălcarea integrității datelor;

   (f) încălcarea confidențialității datelor;

   (g) pierderea disponibilității datelor;

   (h) altele, inclusiv acțiuni cu caracter infracțional.

PARTEA A

Vulnerabilitatea sau metoda de atac asociată amenințărilor

Tabelul A1 cuprinde descrieri de nivel înalt ale amenințărilor și vulnerabilități sau metode de atac asociate acestora.

Tabelul A1

Lista vulnerabilităților sau a metodelor de atac asociate amenințărilor

Descrieri de nivel înalt și de nivel secundar ale vulnerabilității/ amenințărilor			Exemplu de vulnerabilitate sau metodă de atac	
4.3.1. Amenințări privind serverele back-end asociate vehiculelor în circulație	1	Servere back-end utilizate ca mijloc de atacare a unui vehicul sau de extragere a datelor	1.1	Abuz de privilegii de către membrii personalului (atac din interior)
			1.2	Acces neautorizat prin internet la server (activat, de exemplu, de aplicații software de tip „ușă secretă”, de vulnerabilități necorectate ale software-ului sistemului, de atacuri SQL sau prin alte mijloace)
			1.3	Acces fizic neautorizat la server (realizat, de exemplu, cu stick-uri USB sau alte suporturi media conectate la server)
	2	Serviciile furnizate de serverul back-end sunt întrerupte, afectând funcționarea unui vehicul.	2.1	Atacul care vizează serverul back-end oprește funcționarea acestuia, de exemplu îl împiedică să interacționeze cu vehiculele și să ofere serviciile pe care se bazează acestea

Descrieri de nivel înalt și de nivel secundar ale vulnerabilității/ amenințărilor			Exemplu de vulnerabilitate sau metodă de atac	
	3	Datele referitoare la vehicul păstrate pe serverele back-end sunt pierdute sau compromise („încălcarea securității datelor”).	3.1	Abuz de privilegii de către membrii personalului (atac din interior)
			3.2	Pierderea de informații în cloud. Datele sensibile se pot pierde din cauza atacurilor sau a accidentelor atunci când sunt stocate de furnizori terți de servicii de tip cloud
			3.3	Acces neautorizat prin internet la server (activat, de exemplu, de aplicații software de tip „ușă secretă”, de vulnerabilități necorectate ale software-ului sistemului, de atacuri SQL sau prin alte mijloace)
			3.4	Acces fizic neautorizat la server (realizat, de exemplu, cu stick-uri USB sau alte suporturi media conectate la server)
			3.5	Încălcarea securității informațiilor prin partajarea neintenționată a datelor (de exemplu, erori ale administratorilor)
4.3.2. Amenințări la adresa vehiculelor cu privire la canalele de comunicații ale acestora	4	Falsificarea mesajelor sau a datelor primite de vehicul	4.1	Falsificarea mesajelor prin falsuri bazate pe asemănare (de exemplu, mesaje V2X de avertizare cooperativă sau de coordonare a manevrelor, mesaje GNSS etc.)
			4.2	Atac Sybil (pentru a simula prezența altor vehicule ca și cum ar fi multe vehicule pe drum)
	5	Canalele de comunicații utilizate pentru manipulări, ștergeri sau alte modificări neautorizate ale codului/ datelor deținute de vehicul	5.1	Canalele de comunicații permit injectarea de coduri; de exemplu, coduri software binare modificate în mod neautorizat ar putea fi injectate în fluxul de comunicații.
			5.2	Canalele de comunicații permit manipularea datelor/ codului vehiculului
			5.3	Canalele de comunicații permit suprascrierea datelor/codului vehiculului
			5.4	Canalele de comunicații permit ștergerea datelor/ codului vehiculului
			5.5	Canalele de comunicații permit introducerea de date/ coduri în vehicul (scrierea de date/coduri)
	6	Canalele de comunicații permit acceptarea mesajelor care nu prezintă încredere/ nesigure sau care sunt vulnerabile la atacuri de tipul deturnării unei sesiuni/la atacuri prin reluare	6.1	Acceptarea informațiilor dintr-o sursă care nu este fiabilă sau nu este de încredere
			6.2	Atac de tipul „man-in-the-middle”/deturnarea unei sesiuni
			6.3	Atac prin reluare, de exemplu un atac împotriva unui gateway de comunicație permite atacatorului să retrogradeze software-ul unei ECU sau firmware-ul gateway-ului
	7	Informațiile pot fi dezvăluite cu ușurință. De exemplu, prin interceptarea comunicațiilor sau prin accesul neautorizat la fișiere sau directoare sensibile	7.1	Interceptarea informațiilor/radiații interferente/ monitorizarea comunicațiilor
			7.2	Obținerea accesului neautorizat la fișiere sau date

Descrieri de nivel înalt și de nivel secundar ale vulnerabilității/ amenințărilor			Exemplu de vulnerabilitate sau metodă de atac	
	8	Atacuri de tip „blocarea serviciului” prin canale de comunicații pentru a întrerupe funcțiile vehiculului	8.1	Trimiterea unui număr mare de date către sistemul informatic al vehiculului, astfel încât acesta să nu poată furniza servicii în mod obișnuit
			8.2	Atac de tip „gaură neagră”, pentru a întrerupe comunicarea între vehicule, atacatorul putând bloca mesajele între vehicule.
	9	Un utilizator fără privilegii poate obține acces privilegiat la sistemele vehiculului	9.1	Un utilizator fără privilegii poate obține acces privilegiat, de exemplu acces cu drepturi de administrator
	10	Virușii introduși în mediile de comunicații pot infecta sistemele vehiculelor	10.1	Un virus introdus în mediile de comunicații infectează sistemele vehiculelor
	11	Mesajele primite de vehicul (de exemplu, X2V sau mesaje de diagnosticare) sau transmise în interiorul acestuia, includ conținut rău-intenționat	11.1	Mesaje interne rău-intenționate (de exemplu, CAN)
			11.2	Mesaje V2X rău-intenționate, de exemplu, de la infrastructură la vehicul sau de la vehicul la vehicul (de exemplu, CAM, DENM)
			11.3	Mesaje de diagnosticare rău-intenționate
			11.4	Mesaje în format propriu rău-intenționate (de exemplu, cele trimise în mod normal de producătorul de echipamente originale sau de furnizorul de componente/sisteme/funcții)
4.3.3. Amenințări la adresa vehiculelor cu privire la procedurile de actualizare ale acestora	12	Utilizarea greșită sau compromiterea procedurilor de actualizare	12.1	Compromiterea procedurilor de actualizare fără fir a software-ului. Aceasta include contrafacerea programului de actualizare a sistemului sau a firmware-ului
			12.2	Compromiterea procedurilor de actualizare a software-urilor locale/fizice. Aceasta include contrafacerea programului de actualizare a sistemului sau a firmware-ului
			12.3	Software-ul este manipulat înainte de procesul de actualizare (și, prin urmare, este corupt), deși procesul de actualizare este intact
			12.4	Compromiterea cheilor de criptare ale furnizorului de software pentru a permite o actualizare nevalidă
	13	Este posibil refuzul actualizărilor legitime	13.1	Atacurile de tip „blocarea serviciului” împotriva unui server sau a unei rețele de actualizare pentru a împiedica lansarea actualizărilor de software esențiale și/sau deblocarea caracteristicilor specifice clientului
4.3.4. Amenințări la adresa vehiculelor cu privire la acțiunile umane neintenționate care facilitează un atac cibernetic	15	Actorii legitimi pot întreprinde acțiuni care ar facilita, involuntar, un atac cibernetic	15.1	Victima nevinovată (de exemplu, proprietarul, operatorul sau inginerul responsabil de întreținere) este păcălită să întreprindă o acțiune pentru a încărca în mod neintenționat un software rău-intenționat sau pentru a permite un atac
			15.2	Nu sunt respectate procedurile de securitate definite

Descrieri de nivel înalt și de nivel secundar ale vulnerabilității/ amenințărilor			Exemplu de vulnerabilitate sau metodă de atac	
4.3.5. Amenințări la adresa vehiculelor cu privire la conectivitatea și conexiunile externe ale acestora	16	Manipularea conectivității funcțiilor vehiculului permite un atac cibernetic, acesta putând include telematica; sisteme care permit operațiuni la distanță; și sisteme care utilizează comunicații wireless cu rază scurtă de acțiune	16.1	Manipularea funcțiilor concepute pentru a opera sisteme de la distanță, cum ar fi o cheie la distanță, un dispozitiv de imobilizare și o stație de încărcare.
			16.2	Manipularea telematicii vehiculului (de exemplu, manipularea măsurării temperaturii mărfurilor sensibile, deblocarea de la distanță a ușilor de încărcare)
			16.3	Interferența cu sistemele fără fir cu rază scurtă de acțiune sau cu senzorii
	17	Software găzduit produs de terți, de exemplu aplicații de divertisment, utilizate ca mijloace de atac împotriva sistemelor vehiculelor	17.1	Aplicații corupte sau cu nivel redus de securitate, utilizate ca metodă de atacare a sistemelor vehiculului
	18	Dispozitive conectate la interfețe externe, de exemplu porturi USB, un port OBD, utilizate ca mijloc de atac împotriva sistemelor vehiculului	18.1	Interfețe externe precum porturi USB sau de alt tip, utilizate ca punct de atac, de exemplu prin injectarea codului
			18.2	Medii infectate cu un virus conectate la sistemul unui vehicul
			18.3	Acces pentru diagnosticare (de exemplu, chei hardware în portul OBD) utilizat pentru a facilita un atac, de exemplu pentru a manipula parametrii vehiculului (direct sau indirect)
4.3.6. Amenințări la adresa datelor/ codului vehiculelor	19	Extragerea datelor/codului vehiculului	19.1	Extragerea din sistemele vehiculului a unui software protejat de drepturi de autor sau de drepturi de proprietate (piraterie de produse)
			19.2	Acces neautorizat la informațiile confidențiale ale proprietarului, cum ar fi identitatea personală, informații privind contul de plăți, informațiile din agenda de adrese, informații de localizare, identificatorul electronic al vehiculului etc.
			19.3	Extragerea cheilor de criptare
	20	Manipularea datelor/codului vehiculului	20.1	Modificări ilegale/neautorizate ale identificatorului electronic al vehiculului
			20.2	Frauda de identitate. De exemplu, dacă un utilizator dorește să afișeze o altă identitate atunci când comunică cu sistemele de taxare, cu serverul back-end al producătorului
			20.3	Acțiune pentru a eluda sistemele de monitorizare (de exemplu, hacking/manipulare frauduloasă/blocarea mesajelor, cum ar fi datele ODR Tracker sau numărul de rulări)
			20.4	Manipularea datelor pentru falsificarea informațiilor privind conducerea vehiculului (de exemplu, kilometrajul, viteza, indicațiile rutiere etc.)
			20.5	Modificări neautorizate ale datelor de diagnosticare a sistemului
	21	Ștergerea datelor/codului	21.1	Ștergerea/manipularea neautorizată a jurnalelor de evenimente ale sistemului
	22	Introducere de software rău-intenționat	22.2	Introducerea de software rău-intenționat sau de activități ale unui software rău-intenționat

Descrieri de nivel înalt și de nivel secundar ale vulnerabilității/ amenințărilor			Exemplu de vulnerabilitate sau metodă de atac	
	23	Introducerea unui software nou sau suprascrierea unui software existent	23.1	Contrafacerea unui software al sistemului de control al vehiculului sau al sistemului informatic
	24	Întreruperea sistemelor sau a operațiunilor	24.1	Blocarea serviciului, de exemplu, declanșată în rețeaua internă prin inundarea unei magistrale CAN sau prin provocarea unor defecțiuni la o unitate electronică de control prin intermediul unui flux ridicat de mesaje
	25	Manipularea parametrilor vehiculului	25.1	Acces neautorizat pentru falsificarea parametrilor de configurare a funcțiilor-cheie ale vehiculului, cum ar fi datele legate de frână, pragul de declanșare a airbagului etc.
			25.2	Accesul neautorizat pentru falsificarea parametrilor de încărcare, cum ar fi tensiunea de încărcare, puterea de încărcare, temperatura bateriei etc.
4.3.7. Vulnerabilități potențiale care ar putea fi exploatate dacă nu sunt protejate sau reduse suficient	26	Tehnologiile criptografice pot fi compromise sau sunt insuficient aplicate.	26.1	Combinația de chei de criptare scurte și o perioadă lungă de valabilitate permite atacatorului să descifreze criptarea
			26.2	Utilizarea insuficientă a algoritmilor de criptare pentru a proteja sistemele sensibile
			26.3	Utilizarea unor algoritmi de criptare deja perimați sau care vor deveni perimați în curând
	27	Piesele sau consumabilele ar putea fi compromise pentru a permite atacarea vehiculelor	27.1	Hardware sau software proiectat pentru a permite un atac sau nu îndeplinește criteriile de proiectare pentru a opri un atac
	28	Dezvoltarea de software sau hardware permite existența unor vulnerabilități	28.1	Erori de software. Prezența erorilor de software poate constitui o bază pentru potențiale vulnerabilități exploatabile. Acest lucru este valabil mai ales dacă software-ul nu a fost testat pentru a se verifica dacă nu conține un cod cunoscut necorespunzător/erori cunoscute și pentru a reduce riscul prezenței unui cod necorespunzător necunoscut/unor erori necunoscute
			28.2	Utilizarea de elemente reziduale din etapa de dezvoltare (de exemplu, porturi de depanare, porturi JTAG, microprocesoare, certificate de dezvoltare, parole ale dezvoltatorilor etc.) poate permite accesul la unități ECU sau obținerea de privilegii mai mari de către atacatori
	29	Proiectarea rețelei introduce vulnerabilități	29.1	Porturi de internet inutile rămase deschise, care oferă acces la sistemele de rețele
			29.2	Eludarea separării rețelei pentru a obține controlul. Un exemplu specific este utilizarea de gateway-uri neprotejate sau a unor puncte de acces (cum ar fi gateway-urile pentru camioane-remorci), pentru a eluda protecțiile și a obține acces la alte segmente de rețea pentru realizarea de acțiuni rău-intenționate, cum ar fi transmiterea de mesaje arbitrare pe magistrala CAN
	31	Se poate produce un transfer neintenționat de date	31.1	Încălcarea securității informațiilor. Datele cu caracter personal pot fi divulgate atunci când se schimbă utilizatorul autovehiculului (de exemplu, dacă autovehiculul este vândut sau dacă este utilizat ca autovehicul de închiriat și este închiriat unor clienți noi)

Descrieri de nivel înalt și de nivel secundar ale vulnerabilității/ amenințărilor			Exemplu de vulnerabilitate sau metodă de atac	
	32	Manipularea fizică a sistemelor poate permite un atac	32.1	Manipularea hardware-ului electronic, de exemplu hardware electronic neautorizat adăugat la un vehicul pentru a permite un atac de tip „man-in-the-middle” Înlocuirea hardware-ului electronic autorizat (de exemplu, senzori) cu hardware electronic neautorizat Manipularea informațiilor colectate de un senzor (de exemplu, utilizarea unui magnet pentru a deregla senzorul cu efect Hall conectat la cutia de viteze)

PARTEA B

Măsuri de atenuare a amenințărilor ce vizează vehiculele

1. Măsuri de atenuare pentru „canalele de comunicații ale vehiculului”

Măsurile de atenuare a amenințărilor legate de „canalele de comunicații ale vehiculului” sunt enumerate în tabelul B1.

Tabelul B1

Măsuri de atenuare a amenințărilor legate de „canalele de comunicații ale vehiculului”

Referința la tabelul A1	Amenințări la adresa „canalelor de comunicații ale vehiculelor”	Referință	Combatere
4.1	Falsificarea mesajelor (de exemplu, mesaje V2X de avertizare cooperativă sau de coordonare a manevrelor, mesaje GNSS etc.) prin falsuri bazate pe asemănare	M10	Vehiculul trebuie să verifice autenticitatea și integritatea mesajelor pe care le primește
4.2	Atac Sybil (pentru a simula prezența altor vehicule ca și cum ar fi multe vehicule pe drum)	M11	Trebuie implementate controale de securitate pentru stocarea cheilor de criptare (de exemplu, prin utilizarea modulelor de securitate hardware)
5.1	Canalele de comunicații permit injectarea de coduri în datele/codul vehiculului, de exemplu, coduri software binare modificate în mod neautorizat ar putea fi injectate în fluxul de comunicații	M10 M6	Vehiculul trebuie să verifice autenticitatea și integritatea mesajelor pe care le primește Sistemele trebuie să implementeze securitatea încă din etapa de proiectare pentru a reduce la minimum riscurile
5.2	Canalele de comunicații permit manipularea datelor/codului vehiculului	M7	Trebuie aplicate tehnici și modele de control al accesului pentru a proteja datele/codul sistemului
5.3	Canalele de comunicații permit suprascrierea datelor/codului vehiculului		
5.4 21.1	Canalele de comunicații permit ștergerea datelor/codului vehiculului		
5.5	Canalele de comunicații permit introducerea datelor/codului în sistemul vehiculului (scrierea codului de date)		

Referința la tabelul A1	Amenințări la adresa „canalelor de comunicații ale vehiculelor”	Referință	Combatere
6.1	Acceptarea informațiilor dintr-o sursă care nu este fiabilă sau nu este de încredere	M10	Vehiculul trebuie să verifice autenticitatea și integritatea mesajelor pe care le primește
6.2	Atac de tipul „man-in-the-middle”/ deturnarea unei sesiuni	M10	Vehiculul trebuie să verifice autenticitatea și integritatea mesajelor pe care le primește
6.3	Atac prin reluare, de exemplu un atac împotriva unui gateway de comunicație permite atacatorului să retrogradeze software-ul unei ECU sau firmware-ul gateway-ului		
7.1	Interceptarea informațiilor/radiații interferente/monitorizarea comunicațiilor	M12	Datele confidențiale transmise către sau de către vehicul trebuie protejate
7.2	Obținerea accesului neautorizat la fișiere sau date	M8	Prin proiectarea sistemului și controlul accesului, personalul neautorizat nu ar trebui să poată accesa date cu caracter personal sau date critice ale sistemului. Exemple de controale de securitate sunt disponibile în OWASP
8.1	Trimiterea unui număr mare de date către sistemul informatic al vehiculului, astfel încât acesta să nu poată furniza servicii în mod obișnuit	M13	Trebuie folosite măsuri pentru detectarea și recuperarea după un atac de blocare a serviciului
8.2	Atac de tip „gaură neagră”, întreruperea comunicării între vehicule prin blocarea transferului de mesaje către alte vehicule	M13	Trebuie folosite măsuri pentru detectarea și recuperarea după un atac de blocare a serviciului
9.1	Un utilizator fără privilegii poate obține acces privilegiat, de exemplu acces cu drepturi de administrator	M9	Se vor utiliza măsuri de prevenire și detectare a accesului neautorizat
10.1	Un virus introdus în mediile de comunicații infectează sistemele vehiculelor	M14	Trebuie luate în considerare măsuri de protejare a sistemelor împotriva virușilor/aplicațiilor software rău-intenționate introduse
11.1	Mesaje interne rău-intenționate (de exemplu, CAN)	M15	Trebuie luate în considerare măsuri de detectare a mesajelor sau a activităților interne rău-intenționate
11.2	Mesaje V2X rău-intenționate, de exemplu, de la infrastructură la vehicul sau de la vehicul la vehicul (de exemplu, CAM, DENM)	M10	Vehiculul trebuie să verifice autenticitatea și integritatea mesajelor pe care le primește
11.3	Mesaje de diagnosticare rău-intenționate		
11.4	Mesaje în format propriu rău-intenționate (de exemplu, cele trimise în mod normal de producătorul de echipamente originale sau de furnizorul de componente/sisteme/funcții)		

2. Măsuri de atenuare pentru „procesul de actualizare”.

Măsurile de atenuare a amenințărilor legate de „procesul de actualizare” sunt enumerate în tabelul B2.

Tabelul B2

Măsuri de atenuare a amenințărilor legate de „procesul de actualizare”

Referința la tabelul A1	Amenințări la adresa „procesului de actualizare”	Referință	Combatere
12.1	Compromiterea procedurilor de actualizare fără fir a software-ului. Aceasta include contrafacerea programului de actualizare a sistemului sau a firmware-ului	M16	Trebuie folosite proceduri securizate de actualizare a software-ului
12.2	Compromiterea procedurilor de actualizare a software-urilor locale/fizice. Aceasta include contrafacerea programului de actualizare a sistemului sau a firmware-ului		
12.3	Software-ul este manipulat înainte de procesul de actualizare (și, prin urmare, este corupt), deși procesul de actualizare este intact		
12.4	Compromiterea cheilor de criptare ale furnizorului de software pentru a permite o actualizare nevalidă	M11	Trebuie implementate controale de securitate pentru stocarea cheilor de criptare
13.1	Atacurile de tip „blocarea serviciului” împotriva unui server sau a unei rețele de actualizare pentru a împiedica lansarea actualizărilor de software esențiale și/sau deblocarea caracteristicilor specifice clientului	M3	Controalele de securitate se aplică sistemelor back-end. În cazurile în care serverele back-end sunt esențiale pentru furnizarea de servicii, există măsuri de recuperare în caz de întrerupere a funcționării sistemului. Exemple de controale de securitate sunt disponibile în OWASP

3. Măsuri de atenuare pentru „acțiunile umane neintenționate care facilitează un atac cibernetic”

Măsurile de atenuare a amenințărilor legate de „acțiunile umane neintenționate care facilitează un atac cibernetic” sunt enumerate în tabelul B3.

Tabelul B3

Măsurile de atenuare a amenințărilor legate de „acțiunile umane neintenționate care facilitează un atac cibernetic”

Referința la tabelul A1	Amenințări legate de „acțiunile umane neintenționate”	Referință	Combatere
15.1	Victima nevinovată (de exemplu, proprietarul, operatorul sau inginerul responsabil de întreținere) este păcălită să întreprindă o acțiune pentru a încărca în mod neintenționat un software rău-intenționat sau pentru a permite un atac	M18	Se vor implementa măsuri pentru definirea și controlul rolurilor utilizatorilor și a privilegiilor de acces, pe baza principiului privilegiului minim de acces

Referința la tabelul A1	Amenințări legate de „acțiunile umane neintenționate”	Referință	Combatere
15.2	Nu sunt respectate procedurile de securitate definite	M19	Organizațiile trebuie să se asigure că procedurile de securitate sunt definite și respectate, inclusiv în ceea ce privește înregistrarea acțiunilor și accesul la gestionarea funcțiilor de securitate

4. Măsuri de atenuare privind „conectivitatea și conexiunile externe”

Măsurile de atenuare a amenințărilor legate de „conectivitate și conexiunile externe” sunt enumerate în tabelul B4.

Tabelul B4

Măsuri de atenuare a amenințărilor legate de „conectivitate și conexiunile externe”

Referința la tabelul A1	Amenințări privind „conectivitatea și conexiunile externe”	Referință	Combatere
16.1	Manipularea funcțiilor concepute pentru a opera sistemele vehiculului de la distanță, cum ar fi o cheie la distanță, un dispozitiv de imobilizare și o stație de încărcare	M20	Controalele de securitate se aplică sistemelor care au acces la distanță
16.2	Manipularea telematicii vehiculului (de exemplu, manipularea măsurării temperaturii mărfurilor sensibile, deblocarea de la distanță a ușilor de încărcare)		
16.3	Interferența cu sistemele fără fir cu rază scurtă de acțiune sau cu senzorii		
17.1	Aplicații corupte sau cu nivel redus de securitate, utilizate ca metodă de atacare a sistemelor vehiculului	M21	Software-ul trebuie evaluat în ceea ce privește securitatea, autentificat și protejat din punctul de vedere al integrității. Se aplică controale de securitate pentru a reduce la minimum riscul generat de un software terț care este destinat sau preconizat să fie găzduit pe vehicul
18.1	Interfețe externe precum porturi USB sau de alt tip, utilizate ca punct de atac, de exemplu prin injectarea codului	M22	Controalele de securitate se aplică interfețelor externe
18.2	Medii infectate cu viruși conectate la vehicul		
18.3	Acces pentru diagnosticare (de exemplu, chei hardware în portul OBD) utilizat pentru a facilita un atac, de exemplu pentru a manipula parametrii vehiculului (direct sau indirect)	M22	Controalele de securitate se aplică interfețelor externe

5. Măsuri de atenuare privind „țintele potențiale ale unui atac sau motivațiile acestora”

Măsurile de atenuare a amenințărilor legate de „țintele potențiale ale unui atac sau motivațiile acestora” sunt enumerate în tabelul B5.

Tabelul B5

Măsuri de atenuare a amenințărilor legate de „țintele potențiale ale unui atac sau motivațiile acestora”

Referința la tabelul A1	Amenințări privind „țintele potențiale ale unui atac sau motivațiile acestora”	Referință	Combatere
19.1	Extragerea din sistemele vehiculului a unui software protejat de drepturi de autor sau de proprietate (piraterie de produse/furt de software)	M7	Tehnicile și modelele de control al accesului trebuie aplicate pentru a proteja datele/codul sistemului. Exemple de controale de securitate sunt disponibile în OWASP
19.2	Acces neautorizat la informațiile confidențiale ale proprietarului, cum ar fi identitatea personală, informații privind contul de plăți, informațiile din agenda de adrese, informații de localizare, identificatorul electronic al vehiculului etc.	M8	Prin proiectarea sistemului și controlul accesului, personalul neautorizat nu ar trebui să poată accesa date cu caracter personal sau date critice ale sistemului. Exemple de controale de securitate sunt disponibile în OWASP
19.3	Extragerea cheilor de criptare	M11	Trebuie implementate controale de securitate pentru stocarea cheilor de criptare, de exemplu module de securitate
20.1	Modificări ilegale/neautorizate ale identificatorului electronic al vehiculului	M7	Tehnicile și modelele de control al accesului trebuie aplicate pentru a proteja datele/codul sistemului. Exemple de controale de securitate sunt disponibile în OWASP
20.2	Frauda de identitate. De exemplu, dacă un utilizator dorește să afișeze o altă identitate atunci când comunică cu sistemele de taxare, cu serverul back-end al producătorului		
20.3	Acțiune pentru a eluda sistemele de monitorizare (de exemplu, hacking/ manipulare frauduloasă/blocarea mesajelor, cum ar fi datele ODR Tracker sau numărul de rulări)	M7	Tehnicile și modelele de control al accesului trebuie aplicate pentru a proteja datele/codul sistemului. Exemple de controale de securitate sunt disponibile în OWASP Atacurile prin manipularea datelor asupra senzorilor sau a datelor transmise ar putea fi atenuate prin corelarea datelor din diferite surse de informații.
20.4	Manipularea datelor pentru falsificarea informațiilor privind conducerea vehiculului (de exemplu, kilometrajul, viteza, indicațiile rutiere etc.)		
20.5	Modificări neautorizate ale datelor de diagnosticare a sistemului		
21.1	Ștergerea/manipularea neautorizată a jurnalelor de evenimente ale sistemului	M7	Tehnicile și modelele de control al accesului trebuie aplicate pentru a proteja datele/codul sistemului. Exemple de controale de securitate sunt disponibile în OWASP
22.2	Introducerea de software rău-intenționat sau de activități ale unui software rău-intenționat	M7	Tehnicile și modelele de control al accesului trebuie aplicate pentru a proteja datele/codul sistemului. Exemple de controale de securitate sunt disponibile în OWASP
23.1	Contrafacerea unui software al sistemului de control al vehiculului sau al sistemului informatic		

Referința la tabelul A1	Amenințări privind „țintele potențiale ale unui atac sau motivațiile acestora”	Referință	Combatere
24.1	Blocarea serviciului, de exemplu, declanșată în rețeaua internă prin inundarea unei magistrale CAN sau prin provocarea unor defecțiuni la o unitate electronică de control prin intermediul unui flux ridicat de mesaje	M13	Trebuie folosite măsuri pentru detectarea și recuperarea după un atac de blocare a serviciului
25.1	Acces neautorizat pentru falsificarea parametrilor de configurare a funcțiilor-cheie ale vehiculului, cum ar fi datele legate de frână, pragul de declanșare a airbagului etc.	M7	Tehnicile și modelele de control al accesului trebuie aplicate pentru a proteja datele/codul sistemului. Exemple de controale de securitate sunt disponibile în OWASP
25.2	Accesul neautorizat pentru falsificarea parametrilor de încărcare, cum ar fi tensiunea de încărcare, puterea de încărcare, temperatura bateriei etc.		

6. Măsuri de atenuare pentru „vulnerabilități potențiale care ar putea fi exploatate dacă nu sunt protejate sau reduse suficient”

Măsurile de atenuare a amenințărilor legate de „vulnerabilitățile potențiale care ar putea fi exploatate dacă nu sunt protejate sau reduse suficient” sunt enumerate în tabelul B6.

Tabelul B6

Măsuri de atenuare a amenințărilor legate de „vulnerabilitățile potențiale care ar putea fi exploatate dacă nu sunt protejate sau reduse suficient”

Referința la tabelul A1	Amenințări legate de „vulnerabilitățile potențiale care ar putea fi exploatate dacă nu sunt protejate sau reduse suficient”	Referință	Combatere
26.1	Combinația de chei de criptare scurte și o perioadă lungă de valabilitate permite atacatorului să descifreze criptarea	M23	Trebuie respectate cele mai bune practici în materie de securitate cibernetică pentru dezvoltarea de software și hardware
26.2	Utilizarea insuficientă a algoritmilor de criptare pentru a proteja sistemele sensibile		
26.3	Utilizarea unor algoritmi de criptare perimați		
27.1	Hardware sau software proiectat pentru a permite un atac sau care nu îndeplinește criteriile de proiectare pentru a opri un atac	M23	Trebuie respectate cele mai bune practici în materie de securitate cibernetică pentru dezvoltarea de software și hardware
28.1	Prezența erorilor de software poate constitui o bază pentru potențiale vulnerabilități exploatabile. Acest lucru este valabil mai ales dacă software-ul nu a fost testat pentru a se verifica dacă nu conține un cod cunoscut necorespunzător/erori cunoscute și pentru a reduce riscul prezenței unui cod necorespunzător necunoscut/unor erori necunoscute	M23	Trebuie respectate cele mai bune practici în materie de securitate cibernetică pentru dezvoltarea de software și hardware. Testarea securității cibernetice cu acoperire adecvată

Referința la tabelul A1	Amenințări legate de „vulnerabilitățile potențiale care ar putea fi exploatate dacă nu sunt protejate sau reduse suficient”	Referință	Combatere
28.2	Utilizarea de elemente reziduale din etapa de dezvoltare (de exemplu, porturi de depanare, porturi JTAG, microprocesoare, certificate de dezvoltare, parole ale dezvoltatorilor etc.) poate permite accesul la unități ECU sau obținerea de privilegii mai mari de către atacatori		
29.1	Porturi de internet inutile rămase deschise, care oferă acces la sistemele de rețele		
29.2	Eludarea separării rețelei pentru a obține controlul. Un exemplu specific este utilizarea de gateway-uri neprotejate sau a unor puncte de acces (cum ar fi gateway-urile pentru camioane-remorci), pentru a eluda protecțiile și a obține acces la alte segmente de rețea pentru realizarea de acțiuni rău-intenționate, cum ar fi transmiterea de mesaje arbitrare pe magistrala CAN	M23	Trebuie respectate cele mai bune practici în materie de securitate cibernetică pentru dezvoltarea de software și hardware. Trebuie respectate cele mai bune practici în materie de securitate cibernetică pentru proiectarea sistemelor și integrarea în sistem

7. Măsuri de atenuare pentru „pierderea datelor/încălcarea securității datelor de la vehicul”

Măsurile de atenuare a amenințărilor legate de „pierderea datelor/încălcarea securității datelor de la vehicul” sunt enumerate în tabelul B7.

Tabelul B7

Măsurile de atenuare a amenințărilor legate de „pierderea datelor/încălcarea securității datelor de la vehicul”

Referința la tabelul A1	Amenințări privind „pierderea datelor/încălcarea securității datelor de la vehicul”	Referință	Combatere
31.1	Încălcarea securității informațiilor. Securitatea datelor personale poate fi încălcată atunci când se schimbă utilizatorul autovehiculului (de exemplu, autovehiculul este vândut sau este utilizat ca autovehicul de închiriat și este închiriat unor clienți noi)	M24	Se vor respecta cele mai bune practici pentru protecția integrității și confidențialității datelor pentru stocarea datelor cu caracter personal.

8. Măsuri de atenuare pentru „manipularea fizică a sistemelor pentru a permite un atac”

Măsurile de atenuare a amenințărilor legate de „manipularea fizică a sistemelor pentru a permite un atac” sunt enumerate în tabelul B8.

Tabelul B8

Măsuri de atenuare a amenințărilor legate de „manipularea fizică a sistemelor pentru a permite un atac”

Referința la tabelul A1	Amenințări privind „manipularea fizică a sistemelor pentru a permite un atac”	Referință	Combatere
32.1	Manipularea hardware-ului producătorului de echipamente originale, de exemplu hardware neautorizat adăugat la un vehicul pentru a permite un atac de tip „man-in-the-middle”	M9	Se vor utiliza măsuri de prevenire și detectare a accesului neautorizat

PARTEA C

Măsurile de atenuare a amenințărilor în zonele din afara vehiculelor

1. Măsuri de atenuare pentru „serverele back-end”

Măsurile de atenuare a amenințărilor legate de „serverele back-end” sunt enumerate în tabelul C1.

Tabelul C1

Măsuri de atenuare a amenințărilor legate de „serverele back-end”

Referința la tabelul A1	Amenințări pentru „serverele back-end”	Referință	Combatere
1.1 & 3.1	Abuz de privilegii de către membrii personalului (atac din interior)	M1	Controalele de securitate sunt aplicate sistemelor back-end pentru a reduce la minimum riscul de atac din interior
1.2 & 3.3	Acces neautorizat prin internet la server (activat, de exemplu, de aplicații software de tip „ușă secretă”, de vulnerabilități ale software-ului sistemului necorectate, de atacuri SQL sau de alte mijloace)	M2	Controalele de securitate sunt aplicate sistemelor back-end pentru a reduce la minimum riscul de acces neautorizat. Exemple de controale de securitate sunt disponibile în OWASP
1.3 & 3.4	Acces fizic neautorizat la server (realizat, de exemplu, cu stick-uri USB sau alte suporturi media conectate la server)	M8	Prin proiectarea sistemului și controlul accesului, personalul neautorizat nu ar trebui să poată accesa date cu caracter personal sau date critice ale sistemului
2.1	Atacul care vizează serverul back-end oprește funcționarea acestuia, de exemplu îl împiedică să interacționeze cu vehiculele și să ofere serviciile pe care se bazează acestea	M3	Controalele de securitate sunt aplicate sistemelor back-end. În cazurile în care serverele back-end sunt esențiale pentru furnizarea de servicii, există măsuri de recuperare în caz de întrerupere a funcționării sistemului. Exemple de controale de securitate sunt disponibile în OWASP
3.2	Pierderea de informații în cloud. Datele sensibile se pot pierde din cauza atacurilor sau a accidentelor atunci când sunt stocate de furnizori terți de servicii de tip cloud	M4	Se aplică controale de securitate pentru a reduce la minimum riscurile asociate tehnologiei de tip cloud computing. Exemple de controale de securitate sunt disponibile în OWASP și în orientările privind tehnologia de tip cloud computing NCSC
3.5	Încălcarea securității informațiilor prin partajarea neintenționată a datelor (de exemplu, erori ale administratorilor, stocarea datelor în servere aflate în garaje)	M5	Sunt aplicate controale de securitate sistemelor back-end pentru a se preveni încălcarea securității datelor. Exemple de controale de securitate sunt disponibile în OWASP

2. Măsuri de atenuare pentru „acțiunile umane neintenționate”

Măsurile de atenuare a amenințărilor legate de „acțiunile umane neintenționate” sunt enumerate în tabelul C2.

Tabelul C2

Măsurile de atenuare a amenințărilor legate de „acțiunile umane neintenționate”

Referința la tabelul A1	Amenințări legate de „acțiunile umane neintenționate”	Referință	Combatere
15.1	Victima nevinovată (de exemplu, proprietarul, operatorul sau inginerul responsabil de întreținere) este păcălită să întreprindă o acțiune pentru a încărca în mod neintenționat un software rău-intenționat sau pentru a permite un atac	M18	Se vor implementa măsuri pentru definirea și controlul rolurilor utilizatorilor și a privilegiilor de acces, pe baza principiului privilegiului minim de acces
15.2	Nu sunt respectate procedurile de securitate definite	M19	Organizațiile trebuie să se asigure că procedurile de securitate sunt definite și respectate, inclusiv în ceea ce privește înregistrarea acțiunilor și accesul la gestionarea funcțiilor de securitate

3. Măsuri de atenuare pentru „pierderea fizică a datelor”

Măsurile de atenuare a amenințărilor legate de „pierderea fizică a datelor” sunt enumerate în tabelul C3.

Tabelul C3

Măsuri de atenuare a amenințărilor legate de „pierderea fizică a datelor”

Referința la tabelul A1	Amenințări privind „pierderea fizică a datelor”	Referință	Combatere
30.1	Consecințe negative cauzate de o terță parte. Datele sensibile se pot pierde sau pot fi compromise din cauza deteriorării fizice în caz de accident de trafic sau în caz de furt	M24	Se vor respecta cele mai bune practici pentru protecția integrității și confidențialității datelor pentru stocarea datelor cu caracter personal. Exemple de controale de securitate sunt disponibile în ISO/SC27/WG5
30.2	Pierdere generată de conflictele DRM („digital right management” – gestionarea drepturilor digitale). Datele utilizatorului pot fi șterse din cauza problemelor DRM		
30.3	Datele sensibile (sau integritatea acestora) se pot pierde din cauza uzurii fizice a componentelor TI, cauzând potențiale probleme în cascadă (în cazul modificării cheii, de exemplu)		