Regulamin ONZ nr 155 – Jednolite przepisy dotyczące homologacji pojazdów w zakresie cyberbezpieczeństwa i systemu zarządzania bezpieczeństwem [2021/387]

Data wejścia w życie: 22 stycznia 2021 r.

Niniejszy dokument służy wyłącznie do celów dokumentacyjnych. Następujące teksty są autentyczne i prawnie wiążące:

— ECE/TRANS/WP.29/2020/79

— ECE/TRANS/WP.29/2020/94 oraz

— ECE/TRANS/WP.29/2020/97

SPIS TREŚCI

1. ZAKRES

1.1. Niniejszy regulamin ma zastosowanie do pojazdów kategorii M i N w odniesieniu do cyberbezpieczeństwa.

Niniejszy regulamin ma również zastosowanie do pojazdów kategorii O, gdy są one wyposażone w co najmniej jeden elektroniczny moduł sterujący.

1.2. Niniejszy regulamin ma również zastosowanie do pojazdów kategorii L_6 i L_7, jeżeli są one wyposażone w funkcje jazdy zautomatyzowanej, począwszy od poziomu 3, jak określono w dokumencie referencyjnym zawierającym definicje jazdy zautomatyzowanej w ramach WP.29 i w Ogólnych zasadach opracowania regulaminu ONZ w sprawie pojazdów zautomatyzowanych (ECE/TRANS/WP.29/1140).

1.3. Niniejszy regulamin pozostaje bez uszczerbku dla innych regulaminów ONZ oraz regionalnych lub krajowych przepisów regulujących dostęp upoważnionych podmiotów do pojazdu, jego danych, funkcji i zasobów oraz warunki takiego dostępu. Regulamin pozostaje również bez uszczerbku dla stosowania krajowych i regionalnych przepisów dotyczących prywatności i ochrony osób fizycznych w odniesieniu do przetwarzania ich danych osobowych.

1.4. Niniejszy regulamin pozostaje bez uszczerbku dla innych regulaminów ONZ oraz krajowych lub regionalnych przepisów regulujących rozwój i instalację/integrację systemu części zamiennych i komponentów – fizycznych i cyfrowych – w odniesieniu do cyberbezpieczeństwa.

2. DEFINICJE

Do celów niniejszego regulaminu stosuje się następujące definicje:

2.1. „typ pojazdu" oznacza pojazdy, które nie różnią się pod co najmniej następującymi istotnymi względami:

a) oznaczenie typu pojazdu przez producenta;

b) zasadnicze aspekty architektury elektrycznej/elektronicznej i interfejsów zewnętrznych w odniesieniu do cyberbezpieczeństwa;

2.2. „cyberbezpieczeństwo" oznacza stan, w którym pojazdy drogowe i ich funkcje są chronione przed zagrożeniami dla cyberbezpieczeństwa dotyczącymi komponentów elektrycznych lub elektronicznych;

2.3. „system zarządzania cyberbezpieczeństwem" oznacza systematyczne, oparte na analizie ryzyka podejście do ryzyka związanego z zagrożeniami dla cyberbezpieczeństwa pojazdów i ochrony pojazdów przed cyberatakami, w ramach którego definiuje się procesy organizacyjne, obowiązki i zarządzanie;

2.4. „system" oznacza zestaw komponentów lub podsystemów, który realizuje jedną funkcję lub wiele funkcji;

2.5. „etap rozwoju" oznacza okres przed udzieleniem homologacji typu w odniesieniu do określonego typu pojazdu;

2.6. „etap produkcji" odnosi się do czasu trwania produkcji typu pojazdu;

2.7. „etap poprodukcyjny" odnosi się do okresu, w którym typ pojazdu nie jest już produkowany, do czasu wycofania z użytku wszystkich pojazdów tego typu. Pojazdy reprezentujące określony typ pojazdu będą funkcjonowały w trakcie tego etapu, ale nie będą już produkowane. Etap ten kończy się, gdy nie ma już funkcjonujących pojazdów określonego typu;

2.8. „środek ograniczający" oznacza środek ograniczający ryzyko;

2.9. „ryzyko" oznacza możliwość, że dane zagrożenie wykorzysta podatność pojazdu i tym samym spowoduje szkody dla organizacji lub osoby fizycznej;

2.10. „ocena ryzyka" oznacza ogólny proces wyszukiwania, rozpoznawania i opisywania ryzyka (identyfikacja ryzyka), aby zrozumieć charakter ryzyka i określić jego poziom (analiza ryzyka), oraz porównywania wyników analizy ryzyka z kryteriami ryzyka, aby określić, czy dane ryzyko lub jego wielkość są dopuszczalne lub tolerowane (ocena ryzyka);

2.11. „zarządzanie ryzykiem" oznacza skoordynowane działania na rzecz kierowania organizacją i kontrolowania jej w odniesieniu do ryzyka;

2.12. „zagrożenie" oznacza potencjalną przyczynę niepożądanego incydentu, który może skutkować szkodą dla systemu, organizacji lub osoby fizycznej;

2.13. „podatność" oznacza słabość zasobu lub środka ograniczającego, która może zostać wykorzystana przez co najmniej jedno zagrożenie.

3. WYSTĄPIENIE O HOMOLOGACJĘ

3.1. O udzielenie homologacji typu pojazdu w zakresie cyberbezpieczeństwa występuje producent pojazdu lub jego należycie upoważniony przedstawiciel.

3.2. Do wniosku należy dołączyć trzy egzemplarze każdego z niżej wymienionych dokumentów oraz następujące dane:

3.2.1. opis typu pojazdu w odniesieniu do pozycji określonych w załączniku 1 do niniejszego regulaminu;

3.2.2. w przypadkach, w których wykazano, że informacje są objęte prawami własności intelektualnej lub stanowią szczególną wiedzę fachową producenta lub jego dostawców, producent lub jego dostawcy udostępniają informacje wystarczające do umożliwienia odpowiedniego przeprowadzenia kontroli, o których mowa w niniejszym regulaminie. Informacje takie traktuje się w sposób poufny;

3.2.3. świadectwo zgodności dla systemu zarządzania cyberbezpieczeństwem zgodnie z pkt 6 niniejszego regulaminu.

3.3. Dokumentacja dostępna jest w dwóch częściach:

a) pakiet dokumentacji formalnej dotyczącej homologacji, zawierający materiały określone w załączniku 1, który przekazuje się organowi udzielającemu homologacji lub jego upoważnionej placówce technicznej przy składaniu wniosku o udzielenie homologacji typu. Organ udzielający homologacji lub jego upoważniona placówka techniczna wykorzystuje ten pakiet dokumentacji jako podstawowy materiał odniesienia w procesie udzielania homologacji. Organ udzielający homologacji lub jego upoważniona placówka techniczna zapewnia, aby ten pakiet dokumentacji pozostawał dostępny przez co najmniej 10 lat od chwili ostatecznego zaprzestania produkcji danego typu pojazdu;

b) dodatkowe materiały istotne dla spełnienia wymagań określonych w niniejszym regulaminie może zatrzymać producent, ale musi je udostępnić do kontroli przy udzielaniu homologacji typu. Producent zapewnia, aby wszelkie materiały udostępnione do kontroli przy udzielaniu homologacji typu pozostawały dostępne przez okres co najmniej 10 lat od chwili ostatecznego zaprzestania produkcji danego typu pojazdu.

4. OZNAKOWANIE

4.1. Na każdym pojeździe zgodnym z typem pojazdu homologowanym zgodnie z niniejszym regulaminem, w widocznym i łatwo dostępnym miejscu określonym w formularzu homologacji, umieszcza się międzynarodowy znak homologacji zawierający:

4.1.1. okrąg otaczający literę „E”, po której następuje numer identyfikujący państwo udzielające homologacji;

4.1.2. numer niniejszego regulaminu, literę „R”, myślnik i numer homologacji umieszczone po prawej stronie okręgu opisanego w pkt 4.1.1 powyżej.

4.2. Jeżeli pojazd jest zgodny z typem pojazdu homologowanym zgodnie z jednym regulaminem lub większą liczbą regulaminów stanowiących załączniki do Porozumienia w państwie, które udzieliło homologacji na podstawie niniejszego regulaminu, symbol podany w pkt 4.1.1 powyżej nie musi być powtarzany; w takim przypadku numery regulaminów i homologacji oraz dodatkowe symbole wszystkich regulaminów, zgodnie z którymi udzielono homologacji w danym państwie na podstawie niniejszego regulaminu, należy umieścić w kolumnach po prawej stronie symbolu opisanego w pkt 4.1.1 powyżej.

4.3. Znak homologacji musi być czytelny i nieusuwalny.

4.4. Znak homologacji umieszcza się na tabliczce znamionowej pojazdu zamontowanej przez producenta lub w jej pobliżu.

4.5. Przykładowe układy znaku homologacji przedstawiono w załączniku 3 do niniejszego regulaminu.

5. HOMOLOGACJA

5.1. Organy udzielające homologacji udzielają w stosownych przypadkach homologacji typu w odniesieniu do cyberbezpieczeństwa jedynie takim typom pojazdu, które spełniają wymagania określone w niniejszym regulaminie.

5.1.1. Organ udzielający homologacji lub upoważniona placówka techniczna weryfikuje za pomocą kontroli dokumentów, czy producent pojazdów wdrożył niezbędne środki właściwe dla danego typu pojazdu, aby:

a) zebrać i zweryfikować informacje wymagane na podstawie niniejszego regulaminu w całym łańcuchu dostaw, aby wykazać, że zidentyfikowano czynniki ryzyka związane z dostawcą i objęto je zarządzaniem;

b) udokumentować ocenę ryzyka (przeprowadzoną na etapie rozwoju lub z mocą wsteczną), wyniki badań i środki ograniczające zastosowane w odniesieniu do danego typu pojazdu, w tym informacje dotyczące projektu wykorzystane w ocenie ryzyka;

c) wdrożyć odpowiednie środki w zakresie cyberbezpieczeństwa w projekcie typu pojazdu;

d) wykrywać możliwe cyberataki i reagować na nie;

e) rejestrować dane pomagające w wykrywaniu cyberataków i zapewniać zdolności przeprowadzania analizy kryminalistycznej danych, aby umożliwić analizę prób lub udanych cyberataków.

5.1.2. Organ udzielający homologacji lub upoważniona placówka techniczna weryfikuje za pomocą badania pojazdu należącego do danego typu pojazdu, czy producent pojazdów wdrożył środki cyberbezpieczeństwa, które udokumentował. Badania przeprowadza organ udzielający homologacji lub upoważniona placówka techniczna, samodzielnie lub we współpracy z producentem pojazdów, w drodze kontroli wyrywkowej. Kontrola wyrywkowa jest ukierunkowana między innymi na ryzyko, które podczas oceny ryzyka oceniono jako wysokie.

5.1.3. Organ udzielający homologacji lub upoważniona placówka techniczna odmawia udzielenia homologacji typu w odniesieniu do cyberbezpieczeństwa, gdy producent pojazdów nie spełnił co najmniej jednego z wymagań, o których mowa w pkt 7.3, zwłaszcza:

a) producent pojazdów nie przeprowadził wyczerpującej oceny ryzyka, o której mowa w pkt 7.3.3, w tym gdy producent nie rozważył wszystkich czynników ryzyka związanych z zagrożeniami, o których mowa w załączniku 5 część A;

b) producent pojazdów nie chronił typu pojazdu przez czynnikami ryzyka określonymi w ocenie ryzyka przeprowadzonej przez producenta pojazdów lub nie wdrożono proporcjonalnych środków ograniczających wymaganych zgodnie z pkt 7;

c) producent pojazdów nie wdrożył odpowiednich i proporcjonalnych środków w celu zabezpieczenia specjalnych środowisk w danym typie pojazdu (jeśli są zapewnione) do przechowywania i przygotowywania oprogramowania, usług, aplikacji lub danych rynku wtórnego (ang. *aftermarket*);

d) przed udzieleniem homologacji producent pojazdów nie przeprowadził odpowiednich i wystarczających testów w celu sprawdzenia skuteczności wdrożonych środków bezpieczeństwa.

5.1.4. Dokonujący oceny organ udzielający homologacji odmawia również udzielenia homologacji typu w odniesieniu do cyberbezpieczeństwa, gdy organ udzielający homologacji lub upoważniona placówka techniczna nie otrzymały od producenta pojazdów informacji wystarczających do oceny cyberbezpieczeństwa danego typu pojazdu.

5.2. Zawiadomienie o udzieleniu, rozszerzeniu lub odmowie homologacji typu pojazdu na podstawie niniejszego regulaminu należy przesłać Stronom Porozumienia z 1958 r. stosującym niniejszy regulamin na formularzu zgodnym ze wzorem zamieszczonym w załączniku 2 do niniejszego regulaminu.

5.3. Organy udzielające homologacji nie udzielają homologacji typu bez sprawdzenia, czy producent wprowadził satysfakcjonujące ustalenia i procedury na rzecz odpowiedniego zarządzania aspektami cyberbezpieczeństwa objętymi niniejszym regulaminem.

5.3.1. Oprócz kryteriów ustanowionych w załączniku 2 do Porozumienia z 1958 r. organ udzielający homologacji i jego upoważnione placówki techniczne zapewniają dysponowanie:

a) kompetentnym personelem posiadającym odpowiednie umiejętności w zakresie cyberbezpieczeństwa i specjalistyczną wiedzę w zakresie oceny ryzyka w sektorze motoryzacyjnym ([1]);

b) wdrożonymi procedurami dotyczącymi jednolitej oceny zgodnie z niniejszym regulaminem.

([1]) Np. ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.

5.3.2. Każda z Umawiających się Stron, która stosuje niniejszy regulamin, powiadamia i informuje za pośrednictwem swojego organu udzielającego homologacji inne organy udzielające homologacji Umawiających się Stron stosujących niniejszy regulamin ONZ o metodzie i kryteriach przyjętych przez organ notyfikujący za podstawę do oceny odpowiedniości środków wdrożonych zgodnie z niniejszym regulaminem, w szczególności z pkt 5.1, 7.2 i 7.3.

Informacje te udostępnia się a) wyłącznie przed udzieleniem homologacji po raz pierwszy zgodnie z niniejszym regulaminem, oraz b) przy każdej aktualizacji metody lub kryteriów oceny.

Informacje te mają być udostępniane do celów gromadzenia i analizy najlepszych praktyk oraz z myślą o zapewnianiu spójnego stosowania niniejszego regulaminu przez wszystkie organy udzielające homologacji stosujące niniejszy regulamin.

5.3.3. Informacje, o których mowa w pkt 5.3.2 przesyła się w języku angielskim do bezpiecznej internetowej bazy danych DETA ([2]) ustanowionej przez Europejską Komisję Gospodarczą ONZ, w odpowiednim czasie i nie później niż 14 dni przed pierwszym udzieleniem homologacji zgodnie z przedmiotowymi metodami i kryteriami oceny. Informacje te powinny być wystarczające do zrozumienia, jakie minimalne poziomy wydajności przyjął organ udzielający homologacji dla każdego z poszczególnych wymagań, o których mowa w pkt 5.3.2, a także jakie procesy i środki stosuje w celu weryfikacji, czy te minimalne poziomy wydajności są spełnione ([3]).

5.3.4. Organy udzielające homologacji, które otrzymują informacje, o których mowa w pkt 5.3.2, mogą przekazywać uwagi notyfikującemu organowi udzielającemu homologacji, przesyłając je do bazy DETA w ciągu 14 dni od dnia powiadomienia.

5.3.5. Jeśli nie jest możliwe, aby organ udzielający danej homologacji uwzględnił uwagi otrzymane zgodnie z pkt 5.3.4, organy udzielające homologacji, które przesłały uwagi, oraz organ udzielający danej homologacji starają się uzyskać dalsze wyjaśnienia zgodnie z załącznikiem 6 do Porozumienia z 1958 r. Właściwa pomocnicza grupa robocza ([4]) Światowego Forum na rzecz Harmonizacji Przepisów dotyczących Pojazdów (WP.29) do spraw niniejszego regulaminu uzgadnia wspólną interpretację metod i kryteriów oceny ([5]). Ta wspólna interpretacja obowiązuje i wszystkie organy udzielające homologacji wydają odpowiednio homologacje typu na podstawie niniejszego regulaminu.

5.3.6. Każdy z organów udzielających homologacji, który udziela homologacji typu zgodnie z niniejszym regulaminem, powiadamia inne organy udzielające homologacji o udzielonej homologacji. Organ udzielający homologacji przesyła homologację typu wraz z dokumentacją uzupełniającą w języku angielskim do bazy DETA w ciągu 14 dni od dnia udzielenia homologacji ([6]).

5.3.7. Umawiające się Strony mogą analizować udzielone homologacje na podstawie informacji przesłanych zgodnie z pkt 5.3.6. Wszelkie rozbieżności opinii między Umawiającymi się Stronami rozstrzyga się zgodnie z art. 10 i załącznikiem 6 do Porozumienia z 1958 r. Umawiające się Strony informują również właściwą pomocniczą grupę roboczą Światowego Forum na rzecz Harmonizacji Przepisów dotyczących Pojazdów (WP.29) o rozbieżnych interpretacjach w rozumieniu załącznika 6 do Porozumienia z 1958 r. Właściwa grupa robocza pomaga w rozstrzygnięciu rozbieżnych opinii i może w razie potrzeby konsultować się w tej sprawie z WP.29.

5.4. Do celów pkt 7.2 niniejszego regulaminu producent zapewnia wdrożenie aspektów cyberbezpieczeństwa objętych niniejszym regulaminem.

([2]) https://www.unece.org/trans/main/wp29/datasharing.html

([3]) Wytyczne dotyczące szczegółowych informacji (np. metody, kryteriów, poziomu wydajności), które należy przesyłać, oraz formatu zostaną podane w dokumencie interpretacyjnym, który przygotowuje grupa zadaniowa ds. cyberbezpieczeństwa i kwestii bezprzewodowych na potrzeby siódmej sesji GRVA.

([4]) Grupa Robocza ds. Pojazdów Zautomatyzowanych/Autonomicznych i Podłączonych do Internetu (GRVA).

([5]) Interpretacja ta zostanie odzwierciedlona w dokumencie interpretacyjnym, o którym mowa w przypisie do pkt 5.3.3.

([6]) Dalsze informacje dotyczące minimalnych wymagań w zakresie pakietu dokumentacji zostaną opracowane przez GRVA podczas jej siódmej sesji.

6. ŚWIADECTWO ZGODNOŚCI DLA SYSTEMU ZARZĄDZANIA CYBERBEZPIECZEŃSTWEM

6.1. Umawiające się Strony wyznaczają organ udzielający homologacji do przeprowadzenia oceny producenta i wydania świadectwa zgodności dla systemu zarządzania cyberbezpieczeństwem.

6.2. O wydanie świadectwa zgodności dla systemu zarządzania cyberbezpieczeństwem występuje producent pojazdów lub jego należycie upoważniony przedstawiciel.

6.3. Do wniosku należy dołączyć trzy egzemplarze każdego z niżej wymienionych dokumentów oraz następujące dane:

6.3.1. dokumenty opisujące system zarządzania bezpieczeństwem;

6.3.2. podpisana deklaracja z wykorzystaniem wzoru określonego w dodatku 1 do załącznika 1.

6.4. W kontekście oceny producent deklaruje wykorzystanie wzoru określonego w dodatku 1 do załącznika 1 i wykazuje w sposób zadowalający organ udzielający homologacji lub jego upoważnioną placówkę techniczną, że wdrożył procesy niezbędne do spełnienia wszystkich wymagań dotyczących cyberbezpieczeństwa zgodnie z niniejszym regulaminem.

6.5. Po pomyślnym zakończeniu oceny i otrzymaniu od producenta podpisanej deklaracji zgodnie ze wzorem określonym w dodatku 1 do załącznika 1 producentowi przyznaje się świadectwo zwane świadectwem zgodności dla systemu zarządzania cyberbezpieczeństwem, opisane w załączniku 4 do niniejszego regulaminu (zwane dalej „świadectwem zgodności dla systemu zarządzania cyberbezpieczeństwem").

6.6. Organ udzielający homologacji lub jego upoważniona placówka techniczna wykorzystuje wzór określony w załączniku 4 do niniejszego regulaminu do sporządzenia świadectwa zgodności dla systemu zarządzania cyberbezpieczeństwem.

6.7. Świadectwo zgodności dla systemu zarządzania cyberbezpieczeństwem pozostaje ważne przez maksymalnie trzy lata od dnia wydania, chyba że zostanie cofnięte.

6.8. Organ udzielający homologacji, który przyznał świadectwo zgodności dla systemu zarządzania cyberbezpieczeństwem, może w dowolnym momencie sprawdzić, czy wymagania dotyczące wydania tego świadectwa są w dalszym ciągu spełnione. Organ udzielający homologacji cofa świadectwo zgodności dla systemu zarządzania cyberbezpieczeństwem, jeśli wymagania określone w niniejszym regulaminie przestaną być spełnione.

6.9. Producent informuje organ udzielający homologacji lub jego upoważnioną placówkę techniczną o wszelkich zmianach, które będą miały wpływ na adekwatność świadectwa zgodności dla systemu zarządzania cyberbezpieczeństwem. Po konsultacji z producentem organ udzielający homologacji lub jego upoważniona placówka techniczna decydują, czy konieczne są nowe kontrole.

6.10. Producent składa wniosek o wydanie nowego lub przedłużenie ważności istniejącego świadectwa zgodności dla systemu zarządzania cyberbezpieczeństwem z należytym wyprzedzeniem, aby organ udzielający homologacji mógł ukończyć ocenę przed upływem okresu ważności świadectwa zgodności dla systemu zarządzania cyberbezpieczeństwem. Organ udzielający homologacji, pod warunkiem pozytywnej oceny, wydaje nowe świadectwo zgodności dla systemu zarządzania cyberbezpieczeństwem lub przedłuża jego ważność na kolejny okres trzech lat. Organ udzielający homologacji sprawdza, czy system zarządzania cyberbezpieczeństwem w dalszym ciągu spełnia wymagania określone w niniejszym regulaminie. Organ udzielający homologacji wydaje nowe świadectwo w przypadkach, w których poinformowano organ udzielający homologacji lub jego upoważnioną placówkę techniczną o zmianach i zmiany te zostały poddane ponownej ocenie z wynikiem pozytywnym.

6.11. Wygaśnięcie lub cofnięcie świadectwa zgodności dla systemu zarządzania cyberbezpieczeństwem producenta uznaje się – w odniesieniu do typów pojazdów, których dotyczył dany system zarządzania cyberbezpieczeństwem – za zmianę homologacji, o której mowa w pkt 8, która może obejmować cofnięcie homologacji, jeżeli warunki udzielenia homologacji nie są już spełniane.

7. SPECYFIKACJE

7.1. Specyfikacje ogólne

7.1.1. Wymagania określone w niniejszym regulaminie nie ograniczają przepisów ani wymagań określonych w innych regulaminach ONZ.

7.2. Wymagania dotyczące systemu zarządzania cyberbezpieczeństwem

7.2.1. Do celów oceny organ udzielający homologacji lub jego upoważniona placówka techniczna sprawdzają, czy producent pojazdów wdrożył system zarządzania cyberbezpieczeństwem, oraz weryfikują jego zgodność z niniejszym regulaminem.

7.2.2. System zarządzania cyberbezpieczeństwem obejmuje następujące aspekty:

7.2.2.1. producent pojazdów wykazuje organowi udzielającemu homologacji lub upoważnionej placówce technicznej, że jego system zarządzania cyberbezpieczeństwem ma zastosowanie do następujących etapów:

a) etapu rozwoju;

b) etapu produkcji;

c) etapu poprodukcyjnego;

7.2.2.2. producent pojazdów wykazuje, że procesy stosowane w jego systemie zarządzania cyberbezpieczeństwem zapewniają odpowiednie uwzględnienie bezpieczeństwa, w tym czynników ryzyka i środków ograniczających wymienionych w załączniku 5. Należą do nich:

a) procesy wykorzystywane w organizacji producenta do zarządzania cyberbezpieczeństwem;

b) procesy wykorzystywane do identyfikacji czynników ryzyka dla typów pojazdu. W ramach tych procesów uwzględnia się zagrożenia wymienione w załączniku 5 część A oraz inne istotne zagrożenia;

c) procesy wykorzystywane do oceny, kategoryzacji i uwzględniania zidentyfikowanych czynników ryzyka;

d) procesy wprowadzone w celu sprawdzenia, czy zarządzanie zidentyfikowanymi czynnikami ryzyka jest odpowiednie;

e) procesy wykorzystywane do testowania cyberbezpieczeństwa typu pojazdu;

f) procesy wykorzystywane do zapewniania, aby ocena ryzyka była aktualna;

g) procesy wykorzystywane do monitorowania i wykrywania cyberataków, zagrożeń dla cyberbezpieczeństwa i podatności dotyczących typów pojazdu i reagowania na nie oraz procesy wykorzystywane do oceny, czy wdrożone środki na rzecz cyberbezpieczeństwa są w dalszym ciągu skuteczne w świetle nowych zagrożeń dla cyberbezpieczeństwa i podatności, które zidentyfikowano;

h) procesy wykorzystywane do zapewnienia istotnych danych do celów analizy prób lub udanych cyberataków;

7.2.2.3. producent pojazdów wykazuje, że procesy wykorzystywane w jego systemie zarządzania cyberbezpieczeństwem zapewnią, aby – na podstawie kategoryzacji, o której mowa w pkt 7.2.2.2 lit. c) i g) – zagrożenia dla cyberbezpieczeństwa i podatność, które wymagają reakcji producenta pojazdów, były łagodzone w rozsądnych ramach czasowych;

7.2.2.4. producent pojazdów wykazuje, że procesy wykorzystywane w jego systemie zarządzania cyberbezpieczeństwem zapewnią, aby monitorowanie, o którym mowa w pkt 7.2.2.2 lit. g), miało charakter ciągły. Obejmuje ono:

a) pojazdy po pierwszej rejestracji w systemie monitorowania;

b) zdolność do analizowania i wykrywania zagrożeń dla cyberbezpieczeństwa, podatności i cyberataków na podstawie danych dotyczących pojazdów i rejestrów pojazdów. Zdolność ta musi być zgodna z pkt 1.3 i z prawami prywatności właścicieli lub kierowców pojazdów, zwłaszcza w odniesieniu do zgody;

7.2.2.5. od producenta pojazdów wymaga się wykazania, w jaki sposób jego system zarządzania cyberbezpieczeństwem umożliwi zarządzanie potencjalnymi zależnościami między producentem a dostawcami lub usługodawcami, z którymi producent zawarł umowę, lub organizacjami podrzędnymi producenta w odniesieniu do wymagań określonych w pkt 7.2.2.2.

7.3. Wymagania dotyczące typów pojazdu

7.3.1. Producent musi mieć ważne świadectwo zgodności dla systemu zarządzania cyberbezpieczeństwem właściwe dla typu pojazdu, którego dotyczy homologacja.

Jednak w przypadku homologacji typu udzielonych przed dniem 1 lipca 2024 r., jeśli producent pojazdów jest w stanie wykazać, że typ pojazdu nie mógł zostać opracowany zgodnie z systemem zarządzania cyberbezpieczeństwem, producent pojazdów wykazuje, że cyberbezpieczeństwo zostało odpowiednio uwzględnione podczas fazy rozwoju przedmiotowego typu pojazdu.

7.3.2. Producent pojazdów określa w przypadku typu pojazdu, którego dotyczy homologacja, czynniki ryzyka związane z dostawcą i zarządza nimi.

7.3.3. Producent pojazdów określa kluczowe elementy typu pojazdu i przeprowadza wyczerpującą ocenę ryzyka dotyczącą tego typu pojazdu oraz odpowiednio uwzględnia zidentyfikowane czynniki ryzyka lub zarządza nimi. W ocenie ryzyka należy uwzględnić poszczególne elementy typu pojazdu i interakcje między nimi. W ocenie ryzyka należy ponadto uwzględnić interakcje z ewentualnymi systemami zewnętrznymi. Przy ocenie czynników ryzyka producent pojazdów rozważa czynniki ryzyka związane ze wszystkimi zagrożeniami, o których mowa w załączniku 5 część A, a także wszelkie inne istotne czynniki ryzyka.

7.3.4. Producent pojazdów chroni typ pojazdu przez czynnikami ryzyka określonymi w ocenie ryzyka przeprowadzonej przez producenta pojazdów. Wdraża się proporcjonalne środki ograniczające w celu ochrony typu pojazdu. Wdrożone środki ograniczające obejmują wszystkie środki ograniczające, o których mowa w załączniku 5 części B i C, które są istotne dla zidentyfikowanych czynników ryzyka. Jeśli jednak środek ograniczający, o którym mowa w załączniku 5 części B lub C, nie jest istotny lub jest niewystarczający w odniesieniu do określonego ryzyka, producent pojazdów zapewnia wdrożenie innego odpowiedniego środka ograniczającego.

W szczególności w przypadku homologacji typu udzielonych przed dniem 1 lipca 2024 r. producent pojazdów zapewnia wdrożenie innego odpowiedniego środka ograniczającego, jeśli środek ograniczający, o którym mowa w załączniku 5 części B lub C, nie jest wykonalny pod względem technicznym. Producent dostarcza organowi udzielającemu homologacji odpowiednią ocenę wykonalności technicznej.

7.3.5. Producent pojazdów wdraża odpowiednie i proporcjonalne środki w celu zabezpieczenia specjalnych środowisk w danym typie pojazdu (jeśli są zapewnione) do przechowywania i przygotowywania oprogramowania, usług, aplikacji lub danych rynku wtórnego.

7.3.6. Przed udzieleniem homologacji typu producent pojazdów przeprowadza odpowiednie i wystarczające testy w celu sprawdzenia skuteczności wdrożonych środków bezpieczeństwa.

7.3.7. Producent pojazdów wdraża środki dotyczące typu pojazdu, aby:

a) wykrywać cyberataki na pojazdy danego typu i zapobiegać im;

b) wspierać zdolność producenta pojazdów do monitorowania w odniesieniu do wykrywania zagrożeń, podatności i cyberataków istotnych dla danego typu pojazdu;

c) zapewniać zdolności przeprowadzania analizy kryminalistycznej danych w celu umożliwienia analizy prób lub udanych cyberataków.

7.3.8. Kryptograficzne moduły wykorzystywane na potrzeby niniejszego regulaminu muszą być zgodne z normami wynikającymi z konsensusu. Jeżeli stosowane moduły kryptograficzne nie są zgodne z normami wynikającymi z konsensusu, producent pojazdów uzasadnia ich zastosowanie.

7.4. Przepisy dotyczące sprawozdawczości

7.4.1. Producent pojazdów zgłasza organowi udzielającemu homologacji lub upoważnionej placówce technicznej co najmniej raz w roku, lub w stosownych przypadkach częściej, rezultat działań monitorujących zdefiniowanych w pkt 7.2.2.2 lit. g); sprawozdanie takie musi obejmować istotne informacje na temat nowych cyberataków. Producent pojazdów zgłasza również i potwierdza organowi udzielającemu homologacji lub upoważnionej placówce technicznej, że wdrożone w odniesieniu do jego typów pojazdów środki ograniczające w zakresie cyberbezpieczeństwa wciąż funkcjonują, a także zgłasza i potwierdza wszelkie dodatkowe działania, które podjęto.

7.4.2. Organ udzielający homologacji lub upoważniona placówka techniczna weryfikują przekazane informacje oraz, w razie potrzeby, wymagają od producenta pojazdów usunięcia wszelkich wykrytych nieefektywności.

Jeżeli sprawozdawczość lub odpowiedź nie są wystarczające, organ udzielający homologacji może zdecydować o cofnięciu homologacji systemu zarządzania cyberbezpieczeństwem zgodnie z pkt 6.8.

8. ZMIANA TYPU POJAZDU ORAZ ROZSZERZENIE TYPU HOMOLOGACJI

8.1. O każdej zmianie typu pojazdu, która wpływa na jego charakterystykę techniczną w odniesieniu do cyberbezpieczeństwa lub dokumentacji wymaganej w niniejszym regulaminie, należy powiadomić organ udzielający homologacji, który udzielił homologacji typu pojazdu. Organ udzielający homologacji może:

8.1.1. uznać, że wprowadzone zmiany są nadal zgodne z wymaganiami i dokumentacją istniejącej homologacji typu; albo

8.1.2. przejść do niezbędnej oceny uzupełniającej zgodnie z pkt 5 oraz, w stosownych przypadkach, wymagać od upoważnionej placówki technicznej odpowiedzialnej za przeprowadzenie testów przedstawienia sprawozdania z dalszych testów.

8.1.3. O potwierdzeniu, rozszerzeniu lub odmowie udzielenia homologacji, z wyszczególnieniem zmian, informuje się za pośrednictwem formularza zawiadomienia zgodnego ze wzorem zamieszczonym w załączniku 2 do niniejszego regulaminu. Organ udzielający homologacji, który udziela rozszerzenia homologacji, nadaje numer seryjny każdemu takiemu rozszerzeniu i powiadamia o nim pozostałe Strony Porozumienia z 1958 r. stosujące niniejszy regulamin na formularzu zawiadomienia zgodnym ze wzorem przedstawionym w załączniku 2 do niniejszego regulaminu.

9. ZGODNOŚĆ PRODUKCJI

9.1. Procedury zgodności produkcji muszą być zgodne z procedurami określonymi w załączniku 1 do Porozumienia z 1958 r. (E/ECE/TRANS/505/Rev.3) i następującymi wymogami:

9.1.1. posiadacz homologacji zapewnia, aby wyniki badań zgodności produkcji zostały zarejestrowane oraz aby załączone dokumenty pozostały dostępne przez okres ustalony w porozumieniu z organem udzielającym homologacji lub z jego upoważnioną placówką techniczną. Okres ten nie może przekraczać 10 lat od daty ostatecznego zaprzestania produkcji;

9.1.2. organ udzielający homologacji typu, który udzielił homologacji typu, może w dowolnym czasie zweryfikować metody kontroli zgodności stosowane w każdym zakładzie produkcyjnym. Weryfikacji tych dokonuje się zazwyczaj co trzy lata.

10. SANKCJE Z TYTUŁU NIEZGODNOŚCI PRODUKCJI

10.1. Homologacja udzielona w odniesieniu do typu pojazdu zgodnie z niniejszym regulaminem może zostać cofnięta w razie niespełnienia wymagań określonych w niniejszym regulaminie lub jeżeli pojazdy reprezentatywne nie spełniają wymagań określonych w niniejszym regulaminie.

10.2. Jeżeli organ udzielający homologacji postanowi o cofnięciu uprzednio przez siebie udzielonej homologacji, niezwłocznie powiadamia o tym fakcie, na formularzu zawiadomienia zgodnym ze wzorem przedstawionym w załączniku 2 do niniejszego regulaminu, Umawiające się Strony stosujące niniejszy regulamin.

11. OSTATECZNE ZANIECHANIE PRODUKCJI

11.1. Jeżeli posiadacz homologacji ostatecznie zaniecha produkcji typu pojazdu homologowanego zgodnie z niniejszym regulaminem, informuje o tym organ, który udzielił homologacji. Po otrzymaniu stosownego zawiadomienia organ ten powinien poinformować o tym pozostałe Umawiające się Strony Porozumienia stosujące niniejszy regulamin za pomocą kopii formularza homologacji, w którym na końcu umieszczono dużymi literami adnotację „ZANIECHANO PRODUKCJI" opatrzoną podpisem i datą.

12. NAZWY I ADRESY PLACÓWEK TECHNICZNYCH ODPOWIEDZIALNYCH ZA PRZEPROWADZANIE BADAŃ HOMOLOGACYJNYCH ORAZ NAZWY I ADRESY ORGANÓW UDZIELAJĄCYCH HOMOLOGACJI TYPU

12.1. Umawiające się Strony Porozumienia stosujące niniejszy regulamin przekazują sekretariatowi Organizacji Narodów Zjednoczonych nazwy i adresy placówek technicznych odpowiedzialnych za przeprowadzanie badań homologacyjnych oraz organów udzielających homologacji typu, którym należy przesłać wydane w innych krajach zawiadomienia poświadczające udzielenie, rozszerzenie, odmowę udzielenia lub cofnięcie homologacji.

ZAŁĄCZNIK 1

Dokument informacyjny

Poniższe informacje należy dostarczyć, w stosownych przypadkach, w trzech egzemplarzach wraz ze spisem treści. Wszelkie rysunki należy sporządzić w odpowiedniej skali i z dostatecznym stopniem szczegółowości w formacie A4 lub złożone do formatu A4. Ewentualne dołączone fotografie musi cechować wystarczający stopień szczegółowości.

1. Marka (nazwa handlowa producenta): .....

2. Typ i ogólny opis handlowy: .....

3. Sposób identyfikacji typu, jeżeli oznaczono na pojeździe: .....

4. Umiejscowienie tego oznaczenia: .....

5. Kategoria/kategorie pojazdu: .....

6. Nazwa i adres producenta/przedstawiciela producenta: .....

7. Nazwa i adres zakładu montażowego (zakładów montażowych): .....

8. Fotografie lub rysunki reprezentatywnego pojazdu: .....

9. Cyberbezpieczeństwo

9.1. Ogólne cechy konstrukcyjne typu pojazdu, w tym:

a) układy pojazdu istotne z punktu widzenia cyberbezpieczeństwa typu pojazdu;

b) komponenty tych układów istotne z punktu widzenia cyberbezpieczeństwa;

c) interakcje tych układów z innymi układami w typie pojazdu oraz z zewnętrznymi interfejsami.

9.2. Schemat typu pojazdu

9.3. Numer świadectwa zgodności dla systemu zarządzania cyberbezpieczeństwem: .....

9.4. Dokumenty dotyczące typu pojazdu, który ma być homologowany, opisujące rezultat oceny ryzyka pojazdu oraz zidentyfikowanych zagrożeń: .....

9.5. Dokumenty dotyczące typu pojazdu, który ma być homologowany, zawierające opis środków ograniczających wdrożonych w wymienionych układach lub w odniesieniu do typu pojazdu oraz sposobu, w jaki łagodzą one określone czynniki ryzyka: .....

9.6. Dokumenty dotyczące typu pojazdu, który ma być homologowany, zawierające opis zabezpieczenia specjalnych środowisk dotyczących oprogramowania, usług, aplikacji lub danych rynku wtórnego: .....

9.7. Dokumenty dotyczące typu pojazdu, który ma być homologowany, zawierające opis testów zastosowanych w celu weryfikacji cyberbezpieczeństwa typu pojazdu i jego układów, a także wyniki tych testów: .....

9.8. Opis uwzględnienia łańcucha dostaw w odniesieniu do cyberbezpieczeństwa: .....

Dodatek 1 do załącznika 1

Wzór deklaracji producenta dotyczącej zgodności systemu zarządzania cyberbezpieczeństwem

Deklaracja producenta o zgodności z wymaganiami dotyczącymi systemu zarządzania cyberbezpieczeństwem

Nazwa producenta: .....

Adres producenta: .....

..... (*nazwa producenta*) poświadcza, że zainstalowano procesy niezbędne do zapewnienia zgodności z wymaganiami dotyczącymi systemu zarządzania cyberbezpieczeństwem, określonymi w pkt 7.2 regulaminu ONZ nr 155, oraz że będą one utrzymywane..... .....

Sporządzono w ..... (*miejscowość*)

Data: .....

Imię i nazwisko osoby podpisującej: .....

Stanowisko osoby podpisującej: .....

.....

(*pieczęć i podpis przedstawiciela producenta*)

ZAŁĄCZNIK 2

Zawiadomienie

(maksymalny format: A4 (210 × 297 mm))

Wydane przez: Nazwa organu administracji:
.....
.....
.....

Dotyczące (2) udzielenia homologacji
rozszerzenia homologacji
cofnięcia homologacji ze skutkiem od dnia dd/mm/rrrr r.
odmowy udzielenia homologacji
ostatecznego zaniechania produkcji

typu pojazdu zgodnie z regulaminem ONZ nr 155

Nr homologacji: .....

Nr rozszerzenia: .....

Powód rozszerzenia: .....

1. Marka (nazwa handlowa producenta): .....

2. Typ i ogólny opis handlowy: .....

3. Sposób identyfikacji typu, jeżeli oznaczono na pojeździe: .....

3.1. Umiejscowienie tego oznaczenia: .....

4. Kategoria/kategorie pojazdu: .....

5. Nazwa i adres producenta/przedstawiciela producenta: .....

6. Nazwa i adres zakładu produkcji (zakładów produkcji): .....

7. Numer świadectwa zgodności dla systemu zarządzania cyberbezpieczeństwem: .....

8. Upoważniona placówka techniczna odpowiedzialna za przeprowadzenie badań: .....

9. Data sprawozdania z badań: .....

10. Numer sprawozdania z badań: .....

11. Uwagi: (jeżeli są): .....

12. Miejscowość: .....

13. Data: .....

14. Podpis: .....

15. Załączono spis treści pakietu informacyjnego przechowywanego przez organ udzielający homologacji i udostępnianego na wniosek:

([1]) Numer identyfikujący państwo, które udzieliło homologacji/rozszerzyło homologację/odmówiło udzielenia homologacji/cofnęło homologację (zob. przepisy dotyczące homologacji w niniejszym regulaminie).

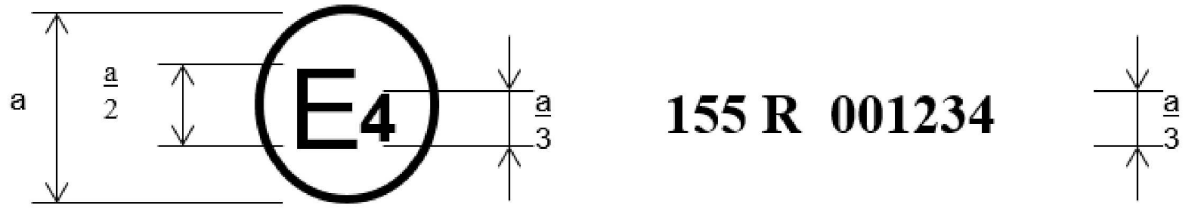
([2]) Niepotrzebne skreślić.:

ZAŁĄCZNIK 3

Układ znaku homologacji

WZÓR A

(zob. pkt 4.2 niniejszego regulaminu)



a = min. 8 mm

Powyższy znak homologacji umieszczony na pojeździe wskazuje, że odnośny typ pojazdu drogowego uzyskał homologację w Niderlandach (E 4) zgodnie z regulaminem nr 155, a numer homologacji to: . Pierwsze dwie cyfry numeru homologacji oznaczają, że homologacji udzielono zgodnie z wymaganiami określonymi w niniejszym regulaminie w jego pierwotnej wersji (00).

ZAŁĄCZNIK 4

Wzór świadectwa zgodności dla systemu zarządzania cyberbezpieczeństwem

Świadectwo zgodności systemu zarządzania cyberbezpieczeństwem

z regulaminem ONZ nr 155

Numer świadectwa [*numer referencyjny*]

[……. *organ udzielający homologacji*]

Zaświadcza, że

Producent: ……

Adres producenta: ……

spełnia przepisy określone w pkt 7.2 regulaminu nr 155

Kontrole następujących elementów: ……

przez (nazwa i adres organu udzielającego homologacji lub placówki technicznej): ……

Numer sprawozdania: ……

Świadectwo jest ważne do dnia [……*data*] r.

Sporządzono w [……*miejscowość*]

Dnia [……*data*] r.

[……*podpis*]

Załączniki: przygotowany przez producenta opis systemu zarządzania cyberbezpieczeństwem

ZAŁĄCZNIK 5

Wykaz zagrożeń i odpowiadających im środków ograniczających

1. Załącznik składa się z pięciu części: W części A niniejszego załącznika opisano zarys zagrożeń, podatności i metod ataku. W części B niniejszego załącznika opisano środki ograniczające zagrożenia, które są planowane dla różnych typów pojazdów. W części C opisano środki ograniczające zagrożenia, które są przeznaczone dla stref znajdujących się poza pojazdami, np. w zapleczu informatycznym.

2. Części A, B i C uwzględnia się do celów oceny i środków ograniczających zagrożenia, które mają zostać wdrożone przez producentów pojazdów.

3. Podatność wysokiego poziomu i związane z nią przykłady zostały załączone w części A. Odniesienia do tych samych załączników zostały wymienione w tabelach w częściach B i C w celu powiązania każdego ataku/podatności z wykazem odpowiednich środków ograniczających zagrożenia.

4. W analizie zagrożeń uwzględnia się również możliwe skutki ataku. Mogą one pomóc w ustaleniu dotkliwości ryzyka i określeniu dodatkowych zagrożeń. Możliwe skutki ataku mogą obejmować:

   a) wpływ na bezpieczne działanie pojazdu;

   b) zatrzymanie funkcji pojazdu;

   c) modyfikację oprogramowania, zmianę działania;

   d) zmianę oprogramowania bez wpływu na działanie;

   e) naruszenie integralności danych;

   f) naruszenie poufności danych;

   g) utratę danych;

   h) inne skutki, w tym o charakterze kryminalnym.

Część A. Podatność lub metoda ataku związane z zagrożeniami

1. W tabeli A1 zamieszczono opisy wysokiego poziomu zagrożeń i związanych z nimi podatności lub metod ataku.

Tabela A1

Wykaz podatności lub metod ataku związanych z zagrożeniami

Opis podatności/zagrożeń wysokiego i niższego poziomu			Przykładowe podatności lub metody ataku	
4.3.1. Zagrożenia dotyczące serwerów wewnętrznych odnoszące się do pojazdów znajdujących się w terenie	1	Serwery wewnętrzne wykorzystywane jako narzędzie do ataku na pojazd lub w celu pobrania danych	1.1	Nadużycie uprawnień przez personel (atak wewnętrzny)
			1.2	Nieuprawniony dostęp internetowy do serwera (umożliwiony na przykład przez *backdoor*, nieusunięte podatności w oprogramowaniu systemu, ataki SQL lub innymi sposobami)
			1.3	Nieuprawniony dostęp fizyczny do serwera (na przykład przez podłączenie pamięci USB lub innego nośnika do serwera)
	2	Zakłócenie połączenia z serwerem wewnętrznym wpływające na działanie pojazdu	2.1	Atak na serwer wewnętrzny powodujący, że serwer przestaje funkcjonować, na przykład uniemożliwiający kontakt z pojazdami i świadczenie usług, od których są one zależne

Opis podatności/zagrożeń wysokiego i niższego poziomu			Przykładowe podatności lub metody ataku	
	3	Utrata lub naruszenie danych dotyczących pojazdów przechowywanych na serwerach wewnętrznych („naruszenie ochrony danych")	3.1	Nadużycie uprawnień przez personel (atak wewnętrzny)
			3.2	Utrata informacji w chmurze. Jeżeli dane są przechowywane przez zewnętrznych dostawców usług w chmurze, w wyniku ataków lub wypadków może dojść do utraty danych wrażliwych
			3.3	Nieuprawniony dostęp internetowy do serwera (umożliwiony na przykład przez *backdoor*, nieusunięte podatności w oprogramowaniu systemu, ataki SQL lub innymi sposobami)
			3.4	Nieuprawniony dostęp fizyczny do serwera (na przykład przez podłączenie pamięci USB lub innego nośnika do serwera)
			3.5	Naruszenie w zakresie informacji przez niezamierzone udostępnienie danych (np. błędy administratora)
4.3.2. Zagrożenia dla pojazdów dotyczące kanałów komunikacyjnych	4	*Spoofing* komunikatów lub danych otrzymywanych przez pojazd	4.1	*Spoofing* komunikatów przez podszycie się (np. 802.11p V2X podczas jazdy w konwoju, komunikaty GNSS itp.)
			4.2	Atak typu Sybil (w celu podszycia się pod inne pojazdy, tak jakby na drodze było wiele pojazdów)
	5	Kanały komunikacji wykorzystywane w celu prowadzenia nieuprawnionej manipulacji kodem/danymi przechowywanymi w pojeździe, ich usunięcia lub wprowadzenia innych zmian	5.1	Kanały komunikacji umożliwiają wstrzyknięcie kodu, na przykład sfałszowane oprogramowanie binarne może zostać wstrzyknięte do strumienia komunikacji
			5.2	Kanały komunikacji umożliwiają manipulowanie danymi/kodem przechowywanymi w pojeździe
			5.3	Kanały komunikacji umożliwiają nadpisanie danych/kodu przechowywanych w pojeździe
			5.4	Kanały komunikacji umożliwiają wymazanie danych/kodu przechowywanych w pojeździe
			5.5	Kanały komunikacji umożliwiają wprowadzenie danych/kodu do pojazdu (wpisanie danych/kodu)
	6	Kanały komunikacji umożliwiają przyjęcie niezaufanych/ niewiarygodnych komunikatów lub są podatne na przechwytywanie sesji/ataki przez powtórzenie	6.1	Przyjmowanie informacji z niewiarygodnego lub niezaufanego źródła
			6.2	Atak typu *man-in-the-middle*/ przechwytywanie sesji
			6.3	Atak przez powtórzenie, na przykład atak na bramkę komunikacji umożliwia atakującemu zmianę oprogramowania elektronicznego modułu sterującego lub oprogramowania układowego bramki na starszą wersję

Opis podatności/zagrożeń wysokiego i niższego poziomu			Przykładowe podatności lub metody ataku	
	7	Informacje można łatwo ujawnić, na przykład podsłuchując komunikaty lub umożliwiając nieuprawniony dostęp do poufnych plików lub folderów	7.1	Przejęcie informacji/zakłócające promieniowanie/monitorowanie komunikatów
			7.2	Uzyskiwanie nieuprawnionego dostępu do plików lub danych
	8	Ataki typu „odmowa usługi" przez kanały komunikacji w celu zakłócenia funkcji pojazdu	8.1	Wysłanie dużej ilości nieprawidłowych danych do systemu informatycznego pojazdu, tak aby nie mógł on świadczyć usług w prawidłowy sposób
			8.2	Atak metodą czarnej dziury – aby zakłócić komunikację między pojazdami, atakujący jest w stanie zablokować komunikaty między pojazdami
	9	Nieuprawniony użytkownik jest w stanie uzyskać uprzywilejowany dostęp do układów pojazdu	9.1	Nieuprawniony użytkownik jest w stanie uzyskać uprzywilejowany dostęp, na przykład dostęp na poziomie administratora
	10	Wirusy osadzone w środkach komunikacji są w stanie zainfekować układy pojazdu	10.1	Wirus osadzony w środkach komunikacji infekuje układy pojazdu
	11	Komunikaty otrzymywane przez pojazd (na przykład X2V lub komunikaty diagnostyczne) lub transmitowane w obrębie pojazdu mają szkodliwą zawartość	11.1	Złośliwe komunikaty wewnętrzne (np. CAN)
			11.2	Złośliwe komunikaty V2X, np. komunikaty infrastruktura–pojazd lub pojazd–pojazd (np. CAM, DENM)
			11.3	Złośliwe komunikaty diagnostyczne
			11.4	Złośliwe komunikaty własne (np. komunikaty wysyłane normalnie z OEM lub przez dostawcę komponentów/ systemu/funkcji)
4.3.3. Zagrożenia dla pojazdów dotyczące ich procedur aktualizacji	12	Nieprawidłowe użycie lub naruszenie procedur aktualizacji	12.1	Naruszenie procedur bezprzewodowej aktualizacji oprogramowania, w tym podrobienie programu lub oprogramowania układowego do aktualizacji systemu
			12.2	Naruszenie procedur lokalnej/fizycznej aktualizacji oprogramowania, w tym podrobienie programu lub oprogramowania układowego do aktualizacji systemu
			12.3	Oprogramowanie jest przedmiotem manipulacji przed procesem aktualizacji (a w związku z tym jest uszkodzone), mimo że proces aktualizacji pozostaje nienaruszony

Opis podatności/zagrożeń wysokiego i niższego poziomu			Przykładowe podatności lub metody ataku	
			12.4	Naruszenie kluczy kryptograficznych dostawcy oprogramowania w celu umożliwienia nieprawidłowej aktualizacji
	13	Możliwość odmowy przeprowadzenia prawidłowej aktualizacji	13.1	Atak typu „odmowa usługi" na serwer lub sieć aktualizacji, aby zapobiec wdrożeniu kluczowych aktualizacji oprogramowania lub odblokować specjalne funkcje klienta
4.3.4. Zagrożenia dla pojazdów związane z niezamierzonymi działaniami człowieka ułatwiającymi cyberataki	15	Uprawnione podmioty mogą bezwiednie podejmować działania ułatwiające przeprowadzenie cyberataku	15.1	Niewinna ofiara (np. właściciel, operator lub inżynier konserwacji) ulega manipulacji i bezwiednie wgrywa złośliwe oprogramowanie lub umożliwia atak
			15.2	Niestosowanie się do zdefiniowanych procedur bezpieczeństwa
4.3.5. Zagrożenia dla pojazdów związane z ich zewnętrzną łącznością i połączeniami	16	Manipulowanie łącznością funkcji pojazdu umożliwia cyberatak; może to obejmować telematykę, systemy umożliwiające zdalne operacje oraz systemy wykorzystujące bezprzewodową komunikację krótkiego zasięgu	16.1	Manipulowanie funkcjami przeznaczonymi na potrzeby zdalnej obsługi układów pojazdu, takimi jak zdalny klucz, immobilizer i stacja ładowania
			16.2	Manipulowanie telematyką pojazdu (np. manipulowanie pomiarami temperatury towarów wrażliwych, zdalne odblokowywanie drzwi ładunkowych)
			16.3	Zakłócenia bezprzewodowych systemów lub czujników krótkiego zasięgu
	17	Zainstalowane oprogramowanie innej firmy, np. aplikacje służące do rozrywki, wykorzystywane jako sposób ataku na układy pojazdu	17.1	Uszkodzone aplikacje lub aplikacje o niskim poziomie bezpieczeństwa oprogramowania wykorzystywane jako metoda ataku na układy pojazdu
	18	Urządzenia podłączone do zewnętrznych interfejsów, np. porty USB, złącze OBD, wykorzystywane jako sposób ataku na układy pojazdu	18.1	Zewnętrzne interfejsy takie jak USB lub inne porty wykorzystywane jako punkt do przeprowadzenia ataku, na przykład przez wstrzyknięcie kodu
			18.2	Media zainfekowane wirusem podłączone do układu pojazdu
			18.3	Dostęp diagnostyczny (np. klucze w złączu OBD) wykorzystywany w celu ułatwienia ataku, np. manipulowanie parametrami pojazdu (bezpośrednio lub pośrednio)
4.3.6. Zagrożenia dla danych/kodów pojazdu	19	Ekstrakcja danych/kodu pojazdu	19.1	Ekstrakcja autorskiego lub własnego oprogramowania z układów pojazdu (piractwo)
			19.2	Nieuprawniony dostęp do prywatnych informacji właściciela, takich jak tożsamość osobista, dane rachunku bankowego, dane z książki adresowej, dane na temat położenia, elektroniczna identyfikacja pojazdu itp.
			19.3	Ekstrakcja kluczy kryptograficznych

Opis podatności/zagrożeń wysokiego i niższego poziomu			Przykładowe podatności lub metody ataku	
	20	Manipulowanie danymi/kodami pojazdu	20.1	Nielegalne/nieuprawnione zmiany elektronicznej identyfikacji pojazdu
			20.2	Oszustwa dotyczące tożsamości. Na przykład, jeżeli użytkownik chce wyświetlić inną tożsamość, komunikując się z systemami poboru opłat drogowych, systemami producenta
			20.3	Działania mające na celu obejście systemów monitorowania (np. włamanie/manipulacja/ blokowanie komunikatów takich jak dane z monitora ODR lub liczba przejazdów)
			20.4	Manipulowanie danymi w celu sfałszowania danych dotyczących przejazdu (np. przebieg, prędkość jazdy, trasa itp.)
			20.5	Nieuprawnione zmiany danych diagnostycznych systemu
	21	Wymazanie danych/kodu	21.1	Nieuprawnione usunięcie dziennika zdarzeń systemu/manipulacja dziennikiem zdarzeń systemu
	22	Wprowadzenie złośliwego oprogramowania	22.2	Wprowadzenie złośliwego oprogramowania lub działania złośliwego oprogramowania
	23	Wprowadzenie nowego oprogramowania lub nadpisanie istniejącego oprogramowania	23.1	Podrobienie oprogramowania systemu sterowania pojazdu lub systemu informatycznego
	24	Zakłócanie systemów lub operacji	24.1	Atak typu „odmowa usługi" – może zostać wywołany na przykład na wewnętrznej sieci przez wprowadzenie wielu komunikatów do magistrali CAN lub przez sprowokowanie wad elektronicznego modułu sterującego poprzez dużą częstotliwość komunikatów
	25	Manipulowanie parametrami pojazdu	25.1	Nieuprawniony dostęp w celu sfałszowania parametrów konfiguracji kluczowych funkcji pojazdu, takich jak dane dotyczące hamulców, progu uruchomienia poduszki powietrznej itp.
			25.2	Nieuprawniony dostęp w celu sfałszowania parametrów ładowania, takich jak napięcie ładowania, moc ładowania, temperatura baterii itp.
4.3.7. Potencjalne podatności, które mogą zostać wykorzystane, jeżeli nie będą wystarczająco chronione lub jeżeli nie zostaną wzmocnione	26	Technologie kryptograficzne mogą zostać naruszone lub nie są wystarczająco stosowane	26.1	Połączenie krótkich kluczy kryptograficznych i długiego okresu ważności pozwala atakującemu na złamanie szyfrowania
			26.2	Niewystarczające wykorzystanie algorytmów kryptograficznych w celu ochrony wrażliwych systemów
			26.3	Stosowanie przestarzałych algorytmów kryptograficznych lub algorytmów kryptograficznych, które wkrótce staną się przestarzałe

Opis podatności/zagrożeń wysokiego i niższego poziomu			Przykładowe podatności lub metody ataku	
	27	Możliwość naruszenia części lub dostaw w celu umożliwienia ataków na pojazdy	27.1	Sprzęt lub oprogramowanie zaprojektowane w sposób umożliwiający przeprowadzenie ataku bądź sprzęt lub oprogramowanie niespełniające kryteriów projektowych dotyczących powstrzymania ataku
	28	Rozwój sprzętu lub oprogramowania umożliwia powstanie podatności	28.1	Błędy w oprogramowaniu Występowanie błędów w oprogramowaniu może stanowić podstawę ewentualnych podatności w zabezpieczeniach, które można wykorzystać Dotyczy to w szczególności sytuacji, w których oprogramowania nie poddano testom mającym na celu weryfikację, czy nie ma w nim znanego błędnego kodu/błędów, oraz ograniczenie ryzyka obecności nieznanego błędnego kodu/błędów
			28.2	Wykorzystanie pozostałości z etapu rozwoju (np. porty debugowania, porty JTAG, mikroprocesory, certyfikaty opracowywania, hasła dewelopera itd.) może umożliwić sprawcy ataku dostęp do elektronicznych modułów sterujących lub uzyskanie wyższych uprawnień
	29	Podatności wprowadzone w projekcie sieci	29.1	Pozostawienie otwartych zbędnych portów internetowych, zapewnienie dostępu do systemów sieci
			29.2	Obejście rozdzielenia sieci w celu uzyskania kontroli Szczególnym przykładem jest wykorzystanie niechronionych bramek lub punktów dostępu (takich jak bramki samochód ciężarowy-przyczepa) w celu obejścia zabezpieczeń i uzyskania dostępu do innych segmentów sieci, aby popełnić czyny dokonywane w złym zamiarze, takie jak wysyłanie arbitralnych komunikatów magistrali CAN
	31	Może wystąpić niezamierzone transferowanie danych	31.1	Naruszenie w zakresie informacji. Możliwość wycieku danych osobowych, kiedy zmienia się użytkownik samochodu (np. samochód zostaje sprzedany lub jest wykorzystywany jako pojazd wynajmowany nowym wynajmującym)
	32	Fizyczne manipulowanie układami może umożliwić atak	32.1	Manipulowanie sprzętem elektronicznym, np. dodanie nieuprawnionego sprzętu elektronicznego do pojazdu w celu umożliwienia ataku typu *man-in-the-middle* Zastąpienie autoryzowanego sprzętu elektronicznego (np. czujników) nieautoryzowanym sprzętem elektronicznym. Manipulowanie informacjami gromadzonymi przez czujnik (na przykład stosowanie magnesu w celu manipulowania czujnikiem wykorzystującym zjawisko Halla połączonym z przekładnią).

Część B. Środki ograniczające zagrożenia dotyczące pojazdów

1. Środki ograniczające zagrożenia związane z „kanałami komunikacji pojazdu"

Środki ograniczające zagrożenia związane z „kanałami komunikacji pojazdu" wymieniono w tabeli B1.

Tabela B1

Środek ograniczający zagrożenia związane z „kanałami komunikacji pojazdu"

Nr w tabeli A1	Zagrożenia dotyczące „kanałów komunikacji pojazdu"	Nr ref.	Środek ograniczający
4.1	Spoofing komunikatów (np. 802.11p V2X podczas jazdy w konwoju, komunikaty GNSS itp.) przez podszycie się	M10	Pojazd weryfikuje autentyczność i integralność komunikatów, które otrzymuje
4.2	Atak typu Sybil (w celu podszycia się pod inne pojazdy, tak jakby na drodze było wiele pojazdów)	M11	Mechanizmy kontroli zabezpieczeń, (np. stosowanie sprzętowych modułów zabezpieczeń), należy wdrażać w odniesieniu do przechowywania kluczy kryptograficznych
5.1	Kanały komunikacji umożliwiają wstrzyknięcie kodu do danych/kodu przechowywanych w pojeździe, na przykład sfałszowane oprogramowanie binarne może zostać wstrzyknięte do strumienia komunikacji	M10 M6	Pojazd weryfikuje autentyczność i integralność komunikatów, które otrzymuje W ramach układów należy wdrażać bezpieczeństwo od etapu projektu w celu minimalizacji ryzyka
5.2	Kanały komunikacji umożliwiają manipulowanie danymi/kodem przechowywanymi w pojeździe	M7	Techniki i projekty w zakresie kontroli dostępu stosuje się w celu ochrony danych/kodu systemu
5.3	Kanały komunikacji umożliwiają nadpisanie danych/kodu przechowywanych w pojeździe		
5.4 21.1	Kanały komunikacji umożliwiają wymazanie danych/kodu przechowywanych w pojeździe		
5.5	Kanały komunikacji umożliwiają wprowadzenie danych/kodu do układów pojazdu (wpisanie danych/kodu)		
6.1	Przyjmowanie informacji z niewiarygodnego lub niezaufanego źródła	M10	Pojazd weryfikuje autentyczność i integralność komunikatów, które otrzymuje
6.2	Atak typu *man-in-the-middle*/ przechwytywanie sesji	M10	Pojazd weryfikuje autentyczność i integralność komunikatów, które otrzymuje
6.3	Atak przez powtórzenie, na przykład atak na bramkę komunikacji umożliwia atakującemu zmianę oprogramowania elektronicznego modułu sterującego lub oprogramowania układowego bramki na starszą wersję		
7.1	Przejęcie informacji/zakłócanie promieniowania/monitorowanie komunikatów	M12	Dane poufne przekazywane do pojazdu lub z pojazdu muszą być chronione
7.2	Uzyskiwanie nieuprawnionego dostępu do plików lub danych	M8	W ramach projektu systemu i kontroli dostępu należy uniemożliwić uzyskanie dostępu do danych osobowych lub danych krytycznych dotyczących systemu przez nieuprawniony personel. Przykład mechanizmów kontroli zabezpieczeń można znaleźć w opracowaniu OWASP

Nr w tabeli A1	Zagrożenia dotyczące „kanałów komunikacji pojazdu”	Nr ref.	Środek ograniczający
8.1	Wysłanie dużej ilości nieprawidłowych danych do systemu informatycznego pojazdu, tak aby nie mógł on świadczyć usług w prawidłowy sposób	M13	Należy wdrożyć środki służące do wykrywania ataku typu „odmowa usługi” i odbudowy po takim ataku
8.2	Atak metodą czarnej dziury, zakłócanie komunikacji między pojazdami przez zablokowanie transferu komunikatów do innych pojazdów	M13	Należy wdrożyć środki służące do wykrywania ataku typu „odmowa usługi” i odbudowy po takim ataku
9.1	Nieuprawniony użytkownik jest w stanie uzyskać uprzywilejowany dostęp, na przykład dostęp na poziomie administratora	M9	Stosuje się środki służące zapobieganiu nieuprawnionemu dostępowi i jego wykrywaniu
10.1	Wirus osadzony w środkach komunikacji infekuje układy pojazdu	M14	Należy wziąć pod uwagę środki służące do ochrony układów przed osadzonymi wirusami/złośliwym oprogramowaniem
11.1	Złośliwe komunikaty wewnętrzne (np. CAN)	M15	Należy wziąć pod uwagę środki służące wykryciu złośliwych komunikatów lub działań wewnętrznych
11.2	Złośliwe komunikaty V2X, np. komunikaty infrastruktura–pojazd lub pojazd–pojazd (np. CAM, DENM)	M10	Pojazd weryfikuje autentyczność i integralność komunikatów, które otrzymuje
11.3	Złośliwe komunikaty diagnostyczne		
11.4	Złośliwe komunikaty własne (np. komunikaty wysyłane normalnie z OEM lub przez dostawcę komponentów/systemu/funkcji)		

2. Środki ograniczające zagrożenia związane z „procesem aktualizacji”

Środki ograniczające zagrożenia związane z „procesem aktualizacji” wymieniono w tabeli B2.

Tabela B2

Środki ograniczające zagrożenia związane z „procesem aktualizacji”

Nr w tabeli A1	Zagrożenia dla „procesu aktualizacji”	Nr ref.	Środek ograniczający
12.1	Naruszenie procedur bezprzewodowej aktualizacji oprogramowania. w tym podrobienie programu lub oprogramowania układowego do aktualizacji systemu	M16	Należy wdrożyć procedury bezpiecznej aktualizacji oprogramowania
12.2	Naruszenie procedur lokalnej/fizycznej aktualizacji oprogramowania. w tym podrobienie programu lub oprogramowania układowego do aktualizacji systemu		
12.3	Oprogramowanie jest przedmiotem manipulacji przed procesem aktualizacji (a w związku z tym jest uszkodzone), mimo że proces aktualizacji pozostaje nienaruszony		

Nr w tabeli A1	Zagrożenia dla „procesu aktualizacji”	Nr ref.	Środek ograniczający
12.4	Naruszenie kluczy kryptograficznych dostawcy oprogramowania w celu umożliwienia nieprawidłowej aktualizacji	M11	Mechanizmy kontroli zabezpieczeń należy wdrażać w odniesieniu do przechowywania kluczy kryptograficznych
13.1	Atak typu „odmowa usługi” na serwer lub sieć aktualizacji, aby zapobiec wdrożeniu kluczowych aktualizacji oprogramowania lub odblokować specjalne funkcje klienta	M3	Wobec systemów zaplecza stosuje się mechanizmy kontroli zabezpieczeń. W przypadku gdy serwery wewnętrzne mają kluczowe znaczenie dla świadczenia usług, w przypadku awarii systemu stosuje się środki naprawcze. Przykłady mechanizmów kontroli zabezpieczeń można znaleźć w opracowaniu OWASP

3. Środki ograniczające zagrożenia związane z „niezamierzonymi działaniami człowieka ułatwiającymi cyberataki”

Środki ograniczające zagrożenia związane z „niezamierzonymi działaniami człowieka ułatwiającymi cyberatak” wymieniono w tabeli B3.

Tabela B3

Środki ograniczające zagrożenia związane z „niezamierzonymi działaniami człowieka ułatwiającymi cyberatak”

Nr w tabeli A1	Zagrożenia związane z „niezamierzonymi działaniami człowieka”	Nr ref.	Środek ograniczający
15.1	Niewinna ofiara (np. właściciel, operator lub inżynier konserwacji) ulega manipulacji i bezwiednie wgrywa złośliwe oprogramowanie lub umożliwia atak	M18	Środki wdraża się w celu zdefiniowania i kontrolowania ról użytkowników i uprawnień dostępu zgodnie z zasadą najmniejszych uprawnień dostępu
15.2	Niestosowanie się do zdefiniowanych procedur bezpieczeństwa	M19	Organizacje zapewniają, aby procedury bezpieczeństwa zostały zdefiniowane i były przestrzegane, w tym aby rejestrowano działania i dostęp w związku z zarządzaniem funkcjami zabezpieczeń

4. Środki ograniczające zagrożenia związane z „zewnętrzną łącznością i połączeniami”

Środki ograniczające zagrożenia związane z zewnętrzną łącznością i połączeniami wymieniono w tabeli B4.

Tabela B4

Środki ograniczające zagrożenia związane z zewnętrzną łącznością i połączeniami

Nr w tabeli A1	Zagrożenia związane z „zewnętrzną łącznością i połączeniami”	Nr ref.	Środek ograniczający
16.1	Manipulowanie funkcjami opracowanymi na potrzeby zdalnej obsługi układów pojazdu, takimi jak zdalny klucz, immobilizer i stacja ładowania	M20	Mechanizmy kontroli zabezpieczeń stosuje się wobec systemów wyposażonych w dostęp zdalny
16.2	Manipulowanie telematyką pojazdu (np. manipulowanie pomiarami temperatury towarów wrażliwych, zdalne odblokowywanie drzwi ładunkowych)		

Nr w tabeli A1	Zagrożenia związane z „zewnętrzną łącznością i połączeniami”	Nr ref.	Środek ograniczający
16.3	Zakłócenia bezprzewodowych systemów lub czujników krótkiego zasięgu		
17.1	Uszkodzone aplikacje lub aplikacje o niskim poziomie bezpieczeństwa oprogramowania wykorzystywane jako metoda ataku na układy pojazdu	M21	Oprogramowanie musi być autoryzowane, poddane ocenie bezpieczeństwa i chronione w zakresie jego integralności Mechanizmy kontroli zabezpieczeń stosuje się w celu zminimalizowania ryzyka związanego z oprogramowaniem zewnętrznym, które ma zostać zainstalowane lub może zostać zainstalowane w pojeździe
18.1	Zewnętrzne interfejsy takie jak USB lub inne porty wykorzystywane jako punkt do przeprowadzenia ataku, na przykład przez wstrzyknięcie kodu	M22	Mechanizmy kontroli zabezpieczeń stosuje się wobec interfejsów zewnętrznych
18.2	Media zainfekowane wirusem podłączone do układu pojazdu		
18.3	Dostęp diagnostyczny (np. klucze w porcie OBD) wykorzystywany w celu ułatwienia ataku, np. manipulowanie parametrami pojazdu (bezpośrednio lub pośrednio)	M22	Mechanizmy kontroli zabezpieczeń stosuje się wobec interfejsów zewnętrznych

5. Środki ograniczające zagrożenia związane z „potencjalnymi celami lub motywami ataku”

Środki ograniczające zagrożenia związane z „potencjalnymi celami lub motywami ataku” wymieniono w tabeli B5.

Tabela B5

Środki ograniczające zagrożenia związane z „potencjalnymi celami lub motywami ataku”

Nr w tabeli A1	Zagrożenia związane z „potencjalnymi celami lub motywami ataku”	Nr ref.	Środek ograniczający
19.1	Ekstrakcja autorskiego lub własnego oprogramowania z układów pojazdu (piractwo/skradzione oprogramowanie)	M7	Techniki i projekty w zakresie kontroli dostępu stosuje się w celu ochrony danych/kodu systemu. Przykłady mechanizmów kontroli zabezpieczeń można znaleźć w opracowaniu OWASP
19.2	Nieuprawniony dostęp do prywatnych informacji właściciela, takich jak tożsamość osobista, dane rachunku bankowego, dane z książki adresowej, dane na temat położenia, elektroniczna identyfikacja pojazdu itp.	M8	W ramach projektu systemu i kontroli dostępu należy uniemożliwić uzyskanie dostępu do danych osobowych lub danych krytycznych dotyczących systemu przez nieuprawniony personel. Przykłady mechanizmów kontroli zabezpieczeń można znaleźć w opracowaniu OWASP
19.3	Ekstrakcja kluczy kryptograficznych	M11	Mechanizmy kontroli zabezpieczeń, np. moduły zabezpieczeń, należy wdrażać w odniesieniu do przechowywania kluczy kryptograficznych
20.1	Nielegalne/nieuprawnione zmiany elektronicznej identyfikacji pojazdu	M7	Techniki i projekty w zakresie kontroli dostępu stosuje się w celu ochrony danych/kodu systemu. Przykłady mechanizmów kontroli zabezpieczeń można znaleźć w opracowaniu OWASP
20.2	Oszustwa dotyczące tożsamości. Na przykład, jeżeli użytkownik chce wyświetlić inną tożsamość, komunikując się z systemami poboru opłat drogowych, systemami producenta		
20.3	Działania mające na celu obejście systemów monitorowania (np. włamanie/ manipulacja/blokowanie komunikatów takich jak dane z monitora ODR lub liczba przejazdów)	M7	Techniki i projekty w zakresie kontroli dostępu stosuje się w celu ochrony danych/kodu systemu. Przykłady mechanizmów kontroli zabezpieczeń można znaleźć w opracowaniu OWASP.

Nr w tabeli A1	Zagrożenia związane z „potencjalnymi celami lub motywami ataku”	Nr ref.	Środek ograniczający
20.4	Manipulowanie danymi w celu sfałszowania danych dotyczących przejazdu (np. przebieg, prędkość jazdy, trasa itp.)		Atakom polegającym na manipulowaniu danymi przeprowadzanym na czujnikach lub przekazywanych danych można zapobiegać poprzez korelację danych z różnych źródeł informacji
20.5	Nieuprawnione zmiany danych diagnostycznych systemu		
21.1	Nieuprawnione usunięcie dziennika zdarzeń systemu/manipulacja dziennikiem zdarzeń systemu	M7	Techniki i projekty w zakresie kontroli dostępu stosuje się w celu ochrony danych/kodu systemu. Przykłady mechanizmów kontroli zabezpieczeń można znaleźć w opracowaniu OWASP.
22.2	Wprowadzenie złośliwego oprogramowania lub działania złośliwego oprogramowania	M7	Techniki i projekty w zakresie kontroli dostępu stosuje się w celu ochrony danych/kodu systemu. Przykłady mechanizmów kontroli zabezpieczeń można znaleźć w opracowaniu OWASP.
23.1	Podrobienie oprogramowania systemu sterowania pojazdu lub systemu informatycznego		
24.1	Atak typu „odmowa usługi” – może zostać wywołany na przykład na wewnętrznej sieci przez wprowadzenie wielu komunikatów do magistrali CAN lub przez sprowokowanie wad elektronicznego modułu sterującego poprzez dużą częstotliwość komunikatów	M13	Należy wdrożyć środki służące do wykrywania ataku typu „odmowa usługi” i odbudowy po takim ataku
25.1	Nieuprawniony dostęp w celu sfałszowania parametrów konfiguracji kluczowych funkcji pojazdu, takich jak dane dotyczące hamulców, progu uruchomienia poduszki powietrznej itp.	M7	Techniki i projekty w zakresie kontroli dostępu stosuje się w celu ochrony danych/kodu systemu. Przykłady mechanizmów kontroli zabezpieczeń można znaleźć w opracowaniu OWASP
25.2	Nieuprawniony dostęp w celu sfałszowania parametrów ładowania, takich jak napięcie ładowania, moc ładowania, temperatura baterii itp.		

6. Środki ograniczające zagrożenia związane z „potencjalnymi podatnościami, które mogą zostać wykorzystane, jeżeli nie będą wystarczająco chronione lub jeżeli nie zostaną wzmocnione”

Środki ograniczające zagrożenia związane z „potencjalnymi podatnościami, które mogą zostać wykorzystane, jeżeli nie będą wystarczająco chronione lub jeżeli nie zostaną wzmocnione”, wymieniono w tabeli B6.

Tabela B6

Środki ograniczające zagrożenia związane z „potencjalnymi podatnościami, które mogą zostać wykorzystane, jeżeli nie będą wystarczająco chronione lub jeżeli nie zostaną wzmocnione”

Nr w tabeli A1	Zagrożenia związane z „potencjalnymi podatnościami, które mogą zostać wykorzystane, jeżeli nie będą wystarczająco chronione lub jeżeli nie zostaną wzmocnione”	Nr ref.	Środek ograniczający
26.1	Połączenie krótkich kluczy kryptograficznych i długiego okresu ważności pozwala atakującemu na złamanie szyfrowania	M23	Stosuje się najlepsze praktyki w zakresie cyberbezpieczeństwa dotyczące rozwoju oprogramowania i sprzętu

Nr w tabeli A1	Zagrożenia związane z „potencjalnymi podatnościami, które mogą zostać wykorzystane, jeżeli nie będą wystarczająco chronione lub jeżeli nie zostaną wzmocnione”	Nr ref.	Środek ograniczający
26.2	Niewystarczające wykorzystanie algorytmów kryptograficznych w celu ochrony wrażliwych systemów		
26.3	Stosowanie przestarzałych algorytmów kryptograficznych		
27.1	Sprzęt lub oprogramowanie zaprojektowane w sposób umożliwiający przeprowadzenie ataku bądź sprzęt lub oprogramowanie niespełniające kryteriów projektowych dotyczących zatrzymania ataku	M23	Stosuje się najlepsze praktyki w zakresie cyberbezpieczeństwa dotyczące rozwoju oprogramowania i sprzętu
28.1	Występowanie błędów w oprogramowaniu może stanowić podstawę ewentualnych podatności, które można wykorzystać Dotyczy to w szczególności sytuacji, w których oprogramowania nie poddano testom mającym na celu weryfikację, czy nie ma w nim znanego błędnego kodu/błędów, oraz ograniczenie ryzyka obecności nieznanego błędnego kodu/błędów	M23	Stosuje się najlepsze praktyki w zakresie cyberbezpieczeństwa dotyczące rozwoju oprogramowania i sprzętu. Testowanie cyberbezpieczeństwa na odpowiednią skalę
28.2	Wykorzystanie pozostałości z etapu rozwoju (np. porty debugowania, porty JTAG, mikroprocesory, certyfikaty opracowywania, hasła dewelopera itd.) może umożliwić sprawcy ataku dostęp do elektronicznych modułów sterujących lub uzyskanie wyższych uprawnień		
29.1	Pozostawienie otwartych zbędnych portów internetowych, zapewnienie dostępu do systemów sieci		
29.2	Obejście rozdzielenia sieci w celu uzyskania kontroli Szczególnym przykładem jest wykorzystanie niechronionych bramek lub punktów dostępu (takich jak bramki samochód ciężarowy-przyczepa) w celu obejścia zabezpieczeń i uzyskania dostępu do innych segmentów sieci, aby popełnić czyny dokonywane w złym zamiarze, takie jak wysyłanie arbitralnych komunikatów magistrali CAN	M23	Stosuje się najlepsze praktyki w zakresie cyberbezpieczeństwa dotyczące rozwoju oprogramowania i sprzętu. Stosuje się najlepsze praktyki w zakresie cyberbezpieczeństwa dotyczące projektu systemu i integracji systemu

7. Środki ograniczające zagrożenia związane z „utratą danych/naruszeniem ochrony danych z pojazdu”

Środki ograniczające zagrożenia związane z „utratą danych/naruszeniem ochrony danych z pojazdu” wymieniono w tabeli B7.

Tabela B7

Środki ograniczające zagrożenia związane z „utratą danych/naruszeniem ochrony danych z pojazdu”

Nr w tabeli A1	Zagrożenia związane z „utratą danych/ naruszeniem ochrony danych z pojazdu”	Nr ref.	Środek ograniczający
31.1	Naruszenie w zakresie informacji. Możliwość naruszenia ochrony danych osobowych, kiedy zmienia się użytkownik samochodu (np. samochód zostaje sprzedany lub jest wykorzystywany jako pojazd wynajmowany nowym najemcom)	M24	Należy przestrzegać najlepszych praktyk służących ochronie integralności i poufności danych w odniesieniu do przechowywania danych osobowych.

8. Środki ograniczające zagrożenia związane z „fizycznym manipulowaniem układami w celu umożliwienia ataku”

Środki ograniczające zagrożenia związane z „fizycznym manipulowaniem układami w celu umożliwienia ataku” wymieniono w tabeli B8.

Tabela B8

Środki ograniczające zagrożenia związane z „fizycznym manipulowaniem układami w celu umożliwienia ataku”

Nr w tabeli A1	Zagrożenia związane z „fizycznym manipulowaniem układami w celu umożliwienia ataku”	Nr ref.	Środek ograniczający
32.1	Manipulowanie sprzętem OEM, np. dodanie nieuprawnionego sprzętu do pojazdu w celu umożliwienia ataku typu *man-in-the-middle*	M9	Stosuje się środki służące zapobieganiu nieuprawnionemu dostępowi i jego wykrywaniu

Część C. Środki ograniczające zagrożenia, które dotyczą obszarów poza pojazdami

1. Środki ograniczające zagrożenia związane z „serwerami wewnętrznymi”

Środki ograniczające zagrożenia związane z „serwerami wewnętrznymi” wymieniono w tabeli C1.

Tabela C1

Środki ograniczające zagrożenia związane z „serwerami wewnętrznymi”

Nr w tabeli A1	Zagrożenia związane z „serwerami wewnętrznymi”	Nr ref.	Środek ograniczający
1.1 i 3.1	Nadużycie uprawnień przez personel (atak wewnętrzny)	M1	Mechanizmy kontroli zabezpieczeń stosuje się do systemów zaplecza w celu zminimalizowania ryzyka ataku wewnętrznego
1.2 i 3.3	Nieuprawniony dostęp internetowy do serwera (umożliwiony na przykład przez *backdoor*, nieusunięte podatności w oprogramowaniu systemu, ataki SQL lub innymi sposobami)	M2	Mechanizmy kontroli zabezpieczeń stosuje się do systemów zaplecza w celu zminimalizowania nieuprawnionego dostępu. Przykłady mechanizmów kontroli zabezpieczeń można znaleźć w opracowaniu OWASP
1.3 i 3.4	Nieuprawniony dostęp fizyczny do serwera (na przykład przez podłączenie pamięci USB lub innego nośnika do serwera)	M8	W ramach projektu systemu i kontroli dostępu należy uniemożliwić uzyskanie dostępu do danych osobowych lub danych krytycznych dotyczących systemu przez nieuprawniony personel
2.1	Atak na serwer wewnętrzny powodujący, że serwer przestaje funkcjonować, na przykład uniemożliwiający kontakt z pojazdami i świadczenie usług, od których są one zależne	M3	Wobec systemów zaplecza stosuje się mechanizmy kontroli zabezpieczeń. W przypadku gdy serwery wewnętrzne mają kluczowe znaczenie dla świadczenia usług, w przypadku awarii systemu stosuje się środki naprawcze. Przykłady mechanizmów kontroli zabezpieczeń można znaleźć w opracowaniu OWASP
3.2	Utrata informacji w chmurze. Jeżeli dane są przechowywane przez zewnętrznych dostawców usług w chmurze, w wyniku ataków lub wypadków może dojść do utraty danych wrażliwych	M4	W celu zminimalizowania ryzyka związanego z przetwarzaniem w chmurze stosuje się mechanizmy kontroli zabezpieczeń. Przykłady mechanizmów kontroli zabezpieczeń można znaleźć w opracowaniu OWASP i wytycznych NCSC dotyczących przetwarzania w chmurze
3.5	Naruszenie w zakresie informacji przez niezamierzone udostępnienie danych (np. błędy administratora, przechowywanie danych ma serwerach w stacjach obsługi)	M5	Mechanizmy kontroli zabezpieczeń stosuje się do systemów zaplecza w celu uniknięcia naruszeń ochrony danych. Przykłady mechanizmów kontroli zabezpieczeń można znaleźć w opracowaniu OWASP

2. Środki ograniczające zagrożenia związane z „niezamierzonymi działaniami człowieka”

Środki ograniczające zagrożenia związane z „niezamierzonymi działaniami człowieka” wymieniono w tabeli C2.

Tabela C2

Środki ograniczające zagrożenia związane z „niezamierzonymi działaniami człowieka”

Nr w tabeli A1	Zagrożenia związane z „niezamierzonymi działaniami człowieka”	Nr ref.	Środek ograniczający
15.1	Niewinna ofiara (np. właściciel, operator lub inżynier konserwacji) ulega manipulacji i bezwiednie wgrywa złośliwe oprogramowanie lub umożliwia atak	M18	Środki wdraża się w celu zdefiniowania i kontrolowania ról użytkowników i uprawnień dostępu zgodnie z zasadą najmniejszych uprawnień dostępu
15.2	Niestosowanie się do zdefiniowanych procedur bezpieczeństwa	M19	Organizacje zapewniają, aby procedury bezpieczeństwa zostały zdefiniowane i były przestrzegane, w tym aby rejestrowano działania i dostęp w związku z zarządzaniem funkcjami zabezpieczeń

3. Środki ograniczające zagrożenia związane z „fizyczną utratą danych”

Środki ograniczające zagrożenia związane z „fizyczną utratą danych” wymieniono w tabeli C3.

Tabela C3

Środki ograniczające zagrożenia związane z „fizyczną utratą danych”

Nr w tabeli A1	Zagrożenia związane z „fizyczną utratą danych”	Nr ref.	Środek ograniczający
30.1	Szkoda spowodowana przez osobę trzecią Do utraty danych wrażliwych lub naruszenia ich ochrony może dojść na skutek fizycznego uszkodzenia w wypadku drogowym lub w przypadku kradzieży	M24	Należy przestrzegać najlepszych praktyk służących ochronie integralności i poufności danych w odniesieniu do przechowywania danych osobowych. Przykłady mechanizmów kontroli zabezpieczeń można znaleźć w ISO/SC27/WG5
30.2	Utrata w wyniku konfliktów DRM (zarządzanie prawami cyfrowym) Dane użytkownika mogą zostać usunięte w wyniku kwestii związanych z DRM		
30.3	Utrata danych wrażliwych (lub ich integralności) może być spowodowana zużyciem komponentów IT, co może mieć skutki kaskadowe (na przykład w przypadku zmiany klucza)		