Předpis OSN č. 155 – Jednotná ustanovení pro schvalování vozidel z hlediska kybernetické bezpečnosti a systému řízení kybernetické bezpečnosti [2021/387]

Datum vstupu v platnost: 22. ledna 2021

Tento dokument slouží výhradně jako dokumentační nástroj. Autentická a právně závazná znění jsou tato:

— ECE/TRANS/WP.29/2020/79

— ECE/TRANS/WP.29/2020/94 a

— ECE/TRANS/WP.29/2020/97

OBSAH

1. OBLAST PŮSOBNOSTI

1.1 Tento předpis se vztahuje na vozidla kategorií M a N, pokud jde o kybernetickou bezpečnost.

Tento předpis se vztahuje rovněž na vozidla kategorie O, pokud jsou vybavena alespoň jednou elektronickou řídicí jednotkou.

1.2 Tento předpis se rovněž vztahuje na vozidla kategorií L_6 a L_7, jsou-li vybavena funkcemi automatizovaného řízení úrovně 3 nebo vyšší, v souladu s referenčním dokumentem s definicemi automatizovaného řízení podle WP.29 a obecnými zásadami pro vypracování předpisu OSN o automatizovaných vozidlech (ECE/TRANS/WP.29/1140).

1.3 Tímto předpisem nejsou dotčeny jiné předpisy OSN, regionální nebo vnitrostátní právní předpisy upravující přístup oprávněných stran k vozidlu, jeho údajům, funkcím a zdrojům a podmínky tohoto přístupu. Rovněž jím není dotčeno uplatňování vnitrostátních a regionálních právních předpisů o soukromí a ochraně fyzických osob v souvislosti se zpracováním jejich osobních údajů.

1.4 Tímto předpisem nejsou dotčeny jiné předpisy OSN, vnitrostátní nebo regionální právní předpisy upravující vývoj a instalaci/začlenění náhradních dílů a součástí, fyzických či digitálních, pokud jde o kybernetickou bezpečnost.

2. DEFINICE

Pro účely tohoto předpisu se rozumí:

2.1 „typem vozidla“, vozidla, která se neliší alespoň v těchto zásadních hlediscích:

a) označení typu vozidla výrobcem;

b) základní aspekty elektrické/elektronické architektury a vnějších rozhraní s ohledem na kybernetickou bezpečnost;

2.2 „kybernetickou bezpečností“ stav, kdy jsou silniční vozidla a jejich funkce chráněny před kybernetickými hrozbami zaměřenými na elektrické nebo elektronické součásti;

2.3 „systémem řízení kybernetické bezpečnosti (CSMS)“ systematický přístup založený na posouzení rizik, který vymezuje organizační procesy, povinnosti a řízení s cílem řešit rizika spojená s kybernetickými hrozbami pro vozidla a chránit vozidla před kybernetickými útoky;

2.4 „systémem“ soubor konstrukčních částí a/nebo subsystémů, které vykonávají jednu nebo více funkcí;

2.5 „vývojovou fází“ doba do schválení typu vozidla;

2.6 „výrobní fází“ doba, po kterou je typ vozidla ve výrobě;

2.7 „povýrobní fází“ doba, po kterou se typ vozidla nevyrábí, ohraničená koncem životnosti všech vozidel daného typu. Vozidla s daného typu budou během této fáze v provozu, nebudou však dále vyráběna. Tato fáze končí, jakmile žádná vozidla konkrétního typu vozidla nejsou v provozu;

2.8 „zmírňujícím opatřením“ kroky ke snížení rizika;

2.9 „rizikem“ potenciál, že zranitelnost vozidla bude zneužita konkrétní hrozbou, čímž bude organizaci nebo jednotlivci způsobena újma;

2.10 „posouzením rizik“ celkový proces zjišťování, rozpoznání a popisu rizik (identifikace rizik) s cílem porozumět povaze rizika a stanovit úroveň rizika (analýza rizik), s následným porovnáním výsledků analýzy rizik s kritérii rizik s cílem určit, zda je riziko a/nebo jeho rozsah přijatelné nebo tolerovatelné (hodnocení rizik);

2.11 „řízením rizik“ koordinované činnosti zaměřené na řízení a kontrolu organizace s ohledem na rizika;

2.12 „hrozbou“ potenciální příčina nežádoucího incidentu, který může vést k poškození systému, organizace nebo jednotlivce;

2.13 „zranitelností“ slabá místa systému nebo zmírňujícího opatření, která mohou být zneužita jednou či více hrozbami.

3. ŽÁDOST O SCHVÁLENÍ

3.1 Žádost o schválení typu vozidla z hlediska kybernetické bezpečnosti předkládá výrobce vozidla nebo jeho řádně pověřený zástupce.

3.2 K žádosti musí být přiloženy následující dokumenty ve trojím vyhotovení a tyto náležitosti:

3.2.1 Popis typu vozidla z hlediska položek uvedených v příloze 1 tohoto předpisu.

3.2.2 V případech, kdy se ukáže, že se na některé informace vztahují práva duševního vlastnictví, nebo pokud tyto informace představují zvláštní know-how výrobce nebo jeho dodavatelů, výrobce nebo jeho dodavatelé poskytnou dostatečné údaje, které umožní řádné provedení kontrol uvedených v tomto předpisu. S těmito informacemi se nakládá jako s důvěrnými.

3.2.3 Osvědčení o shodě pro systém řízení kybernetické bezpečnosti podle bodu 6 tohoto předpisu.

3.3 Dokumentace musí obsahovat dvě části:

a) Soubor formální dokumentace pro schválení obsahující materiál uvedený v příloze 1, který musí být dodán schvalovacímu orgánu nebo jeho technické zkušebně současně při podání žádosti o schválení typu. Tato dokumentace se použije schvalovacím orgánem nebo jeho technickou zkušebnou jako základní reference pro schvalovací proces. Schvalovací orgán nebo jeho technická zkušebna zajistí, aby tato složka dokumentace zůstala k dispozici po dobu nejméně 10 let od okamžiku, kdy je výroba typu vozidla s konečnou platností ukončena;

b) Další podklady, které se vztahují k požadavkům tohoto předpisu, si může výrobce ponechat, musí je však poskytnout ke kontrole při schvalování typu. Výrobce zajistí, aby veškeré materiály, které byly poskytnuty ke kontrole při schválení typu, zůstaly k dispozici po dobu nejméně 10 let od okamžiku, kdy je výroba typu vozidla s konečnou platností ukončena.

4. OZNAČENÍ

4.1 Na každé vozidlo, jež odpovídá typu vozidla schválenému podle tohoto předpisu, se na viditelném a snadno přístupném místě uvedeném na formuláři schválení připevní mezinárodní značka schválení typu, která se skládá z:

4.1.1 písmene „E“ v kružnici, za nímž následuje rozlišovací číslo země, která schválení udělila;

4.1.2 čísla tohoto předpisu, za nímž následuje písmeno „R“, pomlčka a číslo schválení vpravo od kružnice popsané výše v bodě 4.1.1.

4.2 Vyhovuje-li vozidlo typu vozidla schválenému podle jednoho nebo více dalších předpisů připojených k dohodě v zemi, která udělila schválení typu podle tohoto předpisu, není třeba symbol předepsaný výše v bodě 4.1.1 opakovat; v takovém případě se čísla předpisu a schválení, jakož i další symboly všech předpisů, podle kterých bylo schválení uděleno v zemi, která udělila schválení podle tohoto předpisu, umístí do svislých sloupců vpravo od symbolu předepsaného výše v bodě 4.1.1.

4.3 Značka schválení musí být jasně čitelná a nesmazatelná.

4.4 Značka schválení typu se umístí poblíž tabulky s údaji o vozidle, kterou umísťuje výrobce, nebo přímo na ni.

4.5 V příloze 3 tohoto předpisu jsou uvedeny příklady uspořádání značky schválení typu.

5. SCHVÁLENÍ

5.1 Schvalovací orgány v příslušných případech udělí schválení typu z hlediska kybernetické bezpečnosti pouze těm typům vozidel, které splňují požadavky tohoto předpisu.

5.1.1 Schvalovací orgán nebo technická zkušebna kontrolou dokladů ověří, zda výrobce vozidla přijal nezbytná opatření pro daný typ vozidla s cílem:

a) prostřednictvím dodavatelského řetězce shromáždit a ověřit informace požadované tímto předpisem, aby bylo možné prokázat, že rizika spojená s dodavateli jsou identifikována a řízena;

b) popsat posouzení rizik (provedené během vývojové fáze nebo retrospektivně), výsledky zkoušek a zmírňující opatření použitá na typ vozidla, včetně konstrukčních informací, které jsou využité pro posouzení rizik;

c) uplatňovat při návrhu typu vozidla vhodná opatření v oblasti kybernetické bezpečnosti;

d) odhalovat možné útoky v oblasti kybernetické bezpečnosti a reagovat na ně;

e) zaznamenávat údaje na podporu odhalování kybernetických útoků a zajišťovat forenzní zpracování dat pro účely analýzy pokusů o kybernetické útoky a úspěšných kybernetických útoků.

5.1.2 Schvalovací orgán nebo technická zkušebna ověří zkouškou vozidla daného typu vozidla, že výrobce vozidla zavedl opatření kybernetické bezpečnosti, která uvedl v dokumentaci. Zkoušky provádí schvalovací orgán nebo technická zkušebna sama nebo ve spolupráci s výrobcem vozidla výběrem vzorků. Odběr vzorků se zaměří převážně na rizika, která jsou během posouzení rizik vyhodnocena jako vysoká, ale není jimi omezen.

5.1.3 Schvalovací orgán nebo technická zkušebna odmítne udělit schválení typu z hlediska kybernetické bezpečnosti, pokud výrobce vozidla nesplnil jeden nebo více požadavků uvedených v bodě 7.3, zejména:

a) výrobce vozidla neprovedl vyčerpávající posouzení rizik uvedené v bodě 7.3.3; včetně případů, kdy výrobce nezohlednil všechna rizika související s hrozbami uvedenými v příloze 5 části A;

b) výrobce vozidla nechránil typ vozidla před riziky zjištěnými v jeho posouzení rizik, nebo nebyla provedena přiměřená opatření ke zmírnění rizik, jak požaduje bod 7;

c) výrobce vozidel pro daný typ vozidla nezavedl vhodná a přiměřená opatření k zabezpečení vyhrazených prostředí (je-li k dispozici) pro ukládání a spouštění softwaru, služeb, aplikací nebo dat pocházejících z následného trhu;

d) výrobce vozidla neprovedl před schválením vhodné a dostatečné zkoušky k ověření účinnosti zavedených bezpečnostních opatření.

5.1.4 Posuzující schvalovací orgán rovněž odmítne udělit schválení typu z hlediska kybernetické bezpečnosti, pokud schvalovací orgán nebo technická zkušebna neobdržely od výrobce vozidla dostatečné informace pro posouzení kybernetické bezpečnosti typu vozidla.

5.2 Oznámení o schválení nebo o rozšíření či odmítnutí schválení typu vozidla podle tohoto předpisu se zašle stranám dohody z roku 1958, které uplatňují tento předpis, na formuláři podle vzoru v příloze 2 tohoto předpisu.

5.3 Schvalující orgány neudělí schválení typu, aniž by ověřily, že výrobce zavedl uspokojivá opatření a postupy pro řádné řízení aspektů kybernetické bezpečnosti, na něž se vztahuje tento předpis.

5.3.1 Kromě kritérií stanovených v rozpisu 2 k dohodě z roku 1958 musí schvalovací orgán a jeho technické zkušebny zajistit:

a) pracovníky s odpovídající kvalifikací, příslušnými schopnostmi v oblasti kybernetické bezpečnosti a specifickými znalostmi pro posuzování rizika v oblasti automobilového průmyslu ([1]);

b) zavedené postupy pro jednotné hodnocení podle tohoto předpisu.

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

5.3.2 Každá smluvní strana uplatňující tento předpis oznámí a informuje prostřednictvím svého schvalovacího orgánu schvalovací orgány ostatních smluvních stran uplatňujících tento předpis OSN o metodě a kritériích, na jejichž základě oznamující orgán posoudil vhodnost opatření přijatých v souladu s tímto předpisem, a zejména s body 5.1, 7.2 a 7.3.

Tyto informace jsou sdíleny a) pouze před prvním udělením schválení podle tohoto předpisu a b) pokaždé, když dojde k aktualizaci metody nebo kritérií pro posouzení.

Tyto informace mají být sdíleny pro účely shromažďování a analýzy osvědčených postupů a s cílem zajistit konvergentní uplatňování tohoto předpisu všemi schvalovacími orgány, které ho uplatňují.

5.3.3 Informace uvedené v bodě 5.3.2 musí být včas a nejpozději 14 dnů před prvním udělením schválení podle příslušných metod a kritérií posuzování vloženy v anglickém jazyce do zabezpečené internetové databáze DETA ([2]) vytvořené Evropskou hospodářskou komisí OSN. Informace musí být dostatečné k tomu, aby umožnily porozumět minimálním úrovním výkonnosti, které schvalovacím orgánem přijal pro každý konkrétní požadavek uvedený v bodě 5.3.2, jakož i postupům a opatřením, které uplatňuje k ověření, zda jsou tyto minimální úrovně výkonnosti splněny ([3]).

5.3.4 Schvalovací orgány, které obdrží informace uvedené v bodě 5.3.2, mohou podat připomínky oznamujícímu schvalovacímu orgánu tak, že je do 14 dnů ode dne oznámení vloží do databáze DETA.

5.3.5 Není-li možné, aby schvalovací orgán udělující schválení zohlednil připomínky obdržené v souladu s bodem 5.3.4, bude spolu se schvalovacími orgány, které zaslaly připomínky usilovat o další objasnění v souladu s přílohou 6 dohody z roku 1958. Příslušná podpůrná pracovní skupina ([4]) Světového fóra pro harmonizaci předpisů týkajících se vozidel (WP.29) pro účely tohoto předpisu se dohodne na společném výkladu metod a kritérií pro posouzení ([5]). Tento společný výklad se provede a všechny schvalovací orgány budou vydávat schválení typu podle tohoto předpisu v souladu s tímto výkladem.

5.3.6 Každý schvalovací orgán, který uděluje schválení typu podle tohoto předpisu, oznámí udělené schválení ostatním schvalovacím orgánům. Schválení typu spolu s doplňující dokumentací vloží schvalovací orgán do 14 dnů ode dne udělení schválení do databáze DETA v anglickém jazyce ([6]).

5.3.7 Smluvní strany mohou prostudovat udělená schválení na základě informací vložených do databáze DETA podle bodu 5.3.6. V případě rozdílných stanovisek smluvních stran se rozhodne v souladu s článkem 10 a přílohou 6 dohody z roku 1958. Smluvní strany o rozdílných výkladech ve smyslu rozpisu 6 dohody z roku 1958 rovněž informují příslušnou podpůrnou pracovní skupinu Světového fóra pro harmonizaci předpisů týkajících se vozidel (WP.29). Příslušná pracovní skupina přispěje k urovnání rozdílných názorů a v případě potřeby může v této věci konzultovat WP.29.

5.4 Pro účely bodu 7.2 tohoto předpisu výrobce zajistí, aby byly provedeny aspekty kybernetické bezpečnosti, na něž se vztahuje tento předpis.

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

([3]) Pokyny týkající se podrobných informací (např. metody, kritérií, úrovně výkonnosti), které mají být nahrány, a formát se uvedou v interpretačním dokumentu, který připravuje pracovní skupina pracovní skupina pro kybernetickou bezpečnost a otázky bezdrátových přenosů (Task Force on Cyber Security and Over the Air issues), pro sedmé zasedání GRVA.

([4]) Pracovní skupina pro automatizovaná/autonomní a propojená vozidla (GRVA)

([5]) Tento výklad bude zohledněn v interpretačním dokumentu uvedeném v poznámce pod čarou k bodu 5.3.3.

([6]) Další informace o minimálních požadavcích na soubor dokumentace vypracuje skupina GRVA během svého sedmého zasedání.

6. OSVĚDČENÍ O SHODĚ PRO SYSTÉM ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI

6.1 Smluvní strany určí schvalovací orgán, který provede posouzení výrobce a vydá osvědčení o shodě pro CSMS.

6.2 Žádost o schválení typu vozidla z hlediska systému řízení kybernetické bezpečnosti předkládá výrobce vozidla nebo jeho řádně pověřený zástupce.

6.3 K žádosti musí být přiloženy následující dokumenty ve trojím vyhotovení a tyto údaje:

6.3.1 Dokumentace popisující systém řízení kybernetické bezpečnosti.

6.3.2 Podepsané prohlášení podle vzoru popsaného v dodatku 1 k příloze 1.

6.4 V souvislosti s posouzením musí výrobce učinit prohlášení za použití vzoru definovaného v dodatku 1 k příloze 1 a ke spokojenosti schvalovacího orgánu nebo jeho technické zkušebny prokázat, že má nezbytné postupy pro splnění všech požadavků na kybernetickou bezpečnost podle tohoto předpisu.

6.5 Po úspěšném dokončení tohoto posouzení a po obdržení podepsaného prohlášení od výrobce podle vzoru definovaného v dodatku 1 k příloze 1, se výrobci udělí certifikát nazvaný „Certifikát o shodě pro CSMS“, jak je popsán v příloze 4 tohoto předpisu (dále jen „Certifikát o shodě pro CSMS“).

6.6 Schvalovací orgán nebo jeho technická zkušebna použije pro osvědčení o shodě pro CSMS vzor uvedený v příloze 4 tohoto předpisu.

6.7 Osvědčení o shodě pro CSMS zůstává v platnosti po dobu nejvýše tří let ode dne vydání osvědčení, není-li odňato.

6.8 Schvalovací orgán, který udělil certifikát o shodě pro CSMS, může kdykoliv ověřit, že požadavky pro jeho udělení jsou nadále splněny. Schvalovací orgán odejme osvědčení o shodě pro CSMS, pokud požadavky stanovené v tomto předpisu již splněny nejsou.

6.9 Výrobce informuje schvalovací orgán nebo jeho technickou zkušebnu o každé změně, která ovlivní význam osvědčení o shodě pro CSMS. Po konzultaci s výrobcem schvalovací orgán nebo jeho technická zkušebna rozhodne, zda jsou zapotřebí nové kontroly.

6.10 V přiměřené lhůtě, která schvalovacímu orgánu umožní dokončit posouzení před koncem doby platnosti osvědčení o shodě pro CSMS, požádá výrobce o nové osvědčení o shodě pro CSMS nebo o prodloužení stávajícího osvědčení. Schvalovací orgán vydá na základě kladného posouzení nové osvědčení o shodě pro CSMS nebo prodlouží jeho platnost o další tři roky. Schvalovací orgán ověří, že CSMS nadále splňuje požadavky tohoto předpisu. V případě, že byly schvalovacímu orgánu nebo jeho technické zkušebně oznámeny změny a tyto změny byly kladně přehodnoceny, vydá schvalovací orgán nové osvědčení.

6.11 Vypršení platnosti nebo odejmutí osvědčení výrobce o shodě pro CSMS se považuje, vzhledem k typům vozidla, pro které byl dotyčný CSMS relevantní, za změnu schválení podle bodu 8, jejíž součástí může být odejmutí schválení, pokud již podmínky pro udělení schválení nejsou nadále splněny.

7. SPECIFIKACE

7.1 Všeobecné specifikace

7.1.1 Požadavky stanovené tímto předpisem neomezují ustanovení nebo požadavky stanovené jinými předpisy OSN

7.2 Požadavky pro systém řízení kybernetické bezpečnosti

7.2.1 Schvalovací orgán nebo jeho technická zkušebna za účelem posouzení ověří, zda má výrobce vozidla zaveden systém řízení kybernetické bezpečnosti, a ověří jeho soulad s tímto předpisem.

7.2.2 Systém řízení kybernetické bezpečnosti pokrývá následující oblasti:

7.2.2.1 Výrobce vozidla musí schvalovacímu orgánu nebo technické zkušebně prokázat, že jeho systém řízení kybernetické bezpečnosti pokrývá tyto fáze:

a) vývojovou fázi;

b) výrobní fázi;

c) povýrobní fázi.

7.2.2.2 Výrobce vozidla musí prokázat, že postupy používané v jeho systému řízení kybernetické bezpečnosti zajišťují odpovídající zohlednění bezpečnosti, včetně rizik a zmírňujících opatření uvedených v příloze 5. To zahrnuje:

a) procesy používané v rámci organizace výrobce k řízení kybernetické bezpečnosti;

b) procesy používané pro identifikaci rizik pro typy vozidel; V rámci těchto procesů se zvažují hrozby uvedené v příloze 5 části A a další relevantní hrozby;

c) procesy používané pro posouzení, kategorizaci a řešení zjištěných rizik;

d) zavedené postupy k ověření toho, že zjištěná rizika jsou řádně řízena;

e) procesy používané pro testování kybernetické bezpečnosti typu vozidla;

f) procesy používané k zajištění toho, aby posouzení rizik bylo řádně aktualizováno;

g) procesy používané k odhalování a monitorování kybernetických útoků, kybernetických hrozeb a zranitelností na typech vozidel a reakci na ně a postupy používané k posouzení toho, zda jsou zavedená opatření v oblasti kybernetické bezpečnosti stále účinná s ohledem na nově zjištěné kybernetické hrozby a zranitelnosti;

h) procesy používané k poskytování příslušných údajů na podporu analýzy pokusů o kybernetické útoky a úspěšných kybernetických útoků.

7.2.2.3 Výrobce vozidla prokáže, že postupy používané v rámci jeho systému řízení kybernetické bezpečnosti zajistí, aby na základě kategorizace uvedené v bodě 7.2.2.2 písmenu c) a bodě 7.2.2.2 písmenu g) byla pro kybernetické hrozby a zranitelnosti, které vyžadují reakci výrobce vozidla, zmírňující opatření provedena v přiměřené lhůtě.

7.2.2.4 Výrobce vozidla prokáže, že postupy používané v jeho systému řízení kybernetické bezpečnosti zajistí, aby monitorování uvedené v bodě 7.2.2.2 písmenu g) bylo nepřetržité. Toto monitorování musí:

a) zahrnovat vozidla po první registraci;

b) být schopné analyzovat a odhalovat kybernetické hrozby, zranitelnosti a kybernetické útoky na základě údajů o vozidle a protokolů vozidla. Tato schopnost musí být v souladu s bodem 1.3 a právy vlastníků nebo řidičů vozidla na soukromí, zejména pokud jde o souhlas.

7.2.2.5 Výrobce vozidla prokáže, jak bude jeho systém řízení kybernetické bezpečnosti řídit závislosti, které mohou existovat se smluvními dodavateli, poskytovateli služeb nebo podřízenými organizacemi výrobce, pokud jde o požadavky bodu 7.2.2.2.

7.3 Požadavky pro typy vozidel

7.3.1 Výrobce musí mít platné osvědčení o shodě pro systém řízení kybernetické bezpečnosti odpovídající typu vozidla, který se schvaluje.

Pokud však může výrobce v případě schválení typu uděleného před 1. červencem 2024 vozidla prokázat, že typ vozidla nemohl být vyvinut v souladu s CSMS, musí výrobce vozidla prokázat, že během vývojové fáze dotčeného typu vozidla byla kybernetická bezpečnost náležitě zohledněna.

7.3.2 Výrobce vozidla musí u schváleného typu vozidla identifikovat a řídit rizika související s dodavatelem.

7.3.3 Výrobce vozidla musí určit kritické prvky typu vozidla, provést vyčerpávající posouzení rizik pro daný typ vozidla a náležitě řešit zjištěná rizika nebo je řídit. Posouzení rizik zohlední jednotlivé prvky typu vozidla a jejich vzájemné působení. Posouzení rizik dále zohlední interakce s veškerými vnějšími systémy. Při posuzování rizik vezme výrobce vozidla v úvahu rizika související se všemi hrozbami uvedenými v příloze 5 části A, jakož i veškerá další relevantní rizika.

7.3.4 Výrobce vozidla chrání typ vozidla před riziky zjištěnými v jím vypracovaném posouzení rizik. K ochraně typu vozidla musí být provedena přiměřená zmírňující opatření. Provedená opatření ke zmírnění rizik musí zahrnovat všechna zmírnění uvedená v příloze 5 části B a C, která jsou pro zjištěná rizika relevantní. Pokud však zmírnění uvedené v příloze 5 části B nebo C není pro zjištěné riziko relevantní nebo dostatečné, výrobce vozidla zajistí, aby bylo provedeno jiné vhodné zmírnění.

Zejména u schválení typu před 1. červencem 2024 výrobce vozidla zajistí, aby bylo provedeno jiné vhodné zmírnění, pokud zmírňující opatření uvedené v příloze 5 části B nebo C není technicky proveditelné. Příslušné posouzení technické proveditelnosti poskytne výrobce schvalovacímu orgánu.

7.3.5 Výrobce vozidel pro daný typ vozidla zavede vhodná a přiměřená opatření k zabezpečení vyhrazených prostředí (je-li k dispozici) pro ukládání a spouštění softwaru, služeb, aplikací nebo dat pocházejících z následného trhu.

7.3.6 Výrobce vozidla provede před schválením typu vhodné a dostatečné zkoušky k ověření účinnosti zavedených bezpečnostních opatření.

7.3.7 Výrobce vozidla pro typ vozidla provede opatření, jejichž účelem je:

a) odhalovat kybernetické útoky na vozidla typu vozidla a předcházet jim;

b) podporovat schopnost výrobce vozidla provádět monitorování, pokud jde o odhalování hrozeb, zranitelností a kybernetických útoků týkajících se typu vozidla;

c) zajišťovat forenzní zpracování údajů pro účely analýzu pokusů o kybernetické útoky a úspěšných kybernetických útoků.

7.3.8 Kryptografické moduly použité pro účely tohoto předpisu musí být v souladu s normami založenými na konsenzu. Pokud použité kryptografické moduly nejsou v souladu s normami založenými na konsenzu, musí výrobce vozidla jejich použití zdůvodnit.

7.4 Ustanovení o podávání zpráv

7.4.1 V souladu s ustanovením bodu 7.2.2.2 písmene g) podává výrobce vozidla schvalovacímu orgánu nebo technické zkušebně zprávu o výsledcích svých monitorovacích činností, a to včetně příslušných informací o nových kybernetických útocích, nejméně jednou ročně, případně častěji. Výrobce vozidla rovněž potvrdí schvalovacímu orgánu nebo technické zkušebně, že opatření ke zmírnění rizik v oblasti kybernetické bezpečnosti provedená u jejich typů vozidel jsou stále účinná a nahlásí jakákoli další přijatá opatření.

7.4.2 Schvalovací orgán nebo technická zkušebna ověří poskytnuté informace a v případě potřeby požádá výrobce vozidla, aby odstranil nalezené nedostatky.

Není-li podávání zpráv nebo reakce dostačující, může schvalovací orgán rozhodnout o odejmutí CSMS v souladu s bodem 6.8.

8. ZMĚNA TYPU VOZIDLA A ROZŠÍŘENÍ SCHVÁLENÍ TYPU

8.1 Každá změna typu vozidla, která má vliv na jeho technickou výkonnost z hlediska kybernetické bezpečnosti a/nebo dokumentace požadované tímto předpisem, se oznámí schvalovacímu orgánu, který typ vozidla schválil. Tento orgán pak může buď:

8.1.1 dojít k závěru, že změny vyhovují požadavkům a dokumentaci již udělenému schválení typu; nebo

8.1.2 přistoupit k nezbytnému doplňkovému posouzení podle bodu 5 a případně si od technické zkušebny odpovědné za provedení zkoušek vyžádat nový zkušební protokol.

8.1.3 Potvrzení, rozšíření nebo odmítnutí schválení se spolu s výčtem změn sdělí prostřednictvím formuláře sdělení podle vzoru v příloze 2 tohoto předpisu. Schvalovací orgán, který vydává rozšíření schválení, přidělí tomuto rozšíření pořadové číslo a informuje o něm ostatní strany dohody z roku 1958, které uplatňují tento předpis, a to prostřednictvím formuláře sdělení podle vzoru v příloze 2 tohoto předpisu.

9. SHODNOST VÝROBY

9.1 Postupy pro zajištění shodnosti výroby musí odpovídat postupům stanoveným v příloze 1 dohody z roku 1958 (E/ECE/TRANS/505/Rev.3) společně s následujícími požadavky:

9.1.1 Držitel schválení musí zajistit, aby byly výsledky zkoušek shodnosti výroby zaprotokolovány a aby byly připojené dokumenty k dispozici po dobu stanovenou v souladu se schvalovacím orgánem nebo technickou zkušebnou. Tato doba nepřesáhne 10 let od doby, kdy byla výroba definitivně ukončena.

9.1.2 Schvalovací orgán, který udělil schválení typu, může kdykoli ověřit metody kontroly shodnosti používané v každém výrobním zařízení. Obvyklá četnost těchto kontrol je jednou za dva roky.

10. POSTIHY ZA NESHODNOST VÝROBY

10.1 Schválení udělené typu vozidla podle tohoto předpisu je možno odejmout, pokud požadavky stanovené v tomto předpisu nejsou dodrženy nebo jestliže požadavkům tohoto předpisu neodpovídají vozidla vybraná jako vzorek.

10.2 Pokud schvalovací orgán odejme schválení, které dříve udělil, neprodleně to prostřednictvím formuláře sdělení podle vzoru uvedeného v příloze 2 tohoto předpisu oznámí smluvním stranám, které uplatňují tento předpis.

11. DEFINITIVNÍ UKONČENÍ VÝROBY

11.1 Pokud držitel schválení typu zcela ukončí výrobu typu vozidla schváleného podle tohoto předpisu, musí o tom uvědomit orgán, který schválení typu udělil. Po obdržení příslušného sdělení podá uvedený orgán zprávu o ukončení výroby ostatním smluvním stranám dohody, které uplatňují tento předpis, a to prostřednictvím kopie formuláře schválení opatřené na konci velkými písmeny napsanou, podepsanou a datovanou poznámkou „VÝROBA UKONČENA“.

12. NÁZVY A ADRESY TECHNICKÝCH ZKUŠEBEN ODPOVĚDNÝCH ZA PROVÁDĚNÍ SCHVALOVACÍ ZKOUŠKY A NÁZVY A ADRESY SCHVALOVACÍCH ORGÁNŮ

12.1 Smluvní strany dohody, které uplatňují tento předpis, sdělí sekretariátu Organizace spojených národů názvy a adresy technických zkušeben odpovědných za provádění schvalovacích zkoušek, jakož i názvy a adresy schvalovacích orgánů, které schválení udělují a jimž se mají zasílat formuláře osvědčující udělení, rozšíření, zamítnutí nebo odnětí schválení vydané v jiných zemích.

PŘÍLOHA 1

Informační dokument

Následující informace, přicházejí-li v úvahu, se spolu se soupisem obsahu předkládají trojmo. Předkládají-li se výkresy, musí být dodány ve vhodném měřítku a s dostatečnými podrobnostmi na archu formátu A4, nebo musí být na tento formát složeny. Fotografie, pokud se přikládají k žádosti, musí být dostatečně detailní.

1. Značka (obchodní název výrobce): .....

2. Typ a všeobecný obchodní popis: .....

3. Způsob označení typu, je-li na vozidle vyznačen: .....

4. Umístění tohoto označení: .....

5. Kategorie vozidla: .....

6. Jméno a adresa výrobce/zástupce výrobce: .....

7. Název (názvy) a adresa (adresy) montážního závodu (závodů): .....

8. Fotografie a/nebo výkres (výkresy) reprezentujícího vozidla: .....

9. Kybernetická bezpečnost

9.1 Obecné konstrukční vlastnosti typu vozidla, včetně:

a) systémů vozidla, které jsou důležité pro kybernetickou bezpečnost typu vozidla;

b) konstrukčních částí těchto systémů, které jsou relevantní pro kybernetickou bezpečnost;

c) vzájemného působení těchto systémů s jinými systémy v rámci typu vozidla a s vnějšími rozhraními.

9.2 Schematické znázornění typu vozidla

9.3 Číslo osvědčení o shodě pro CSMS .....

9.4 Dokumentace pro typ vozidla, který má být schválen, popisující výsledek jeho posouzení rizik a zjištěná rizika: .....

9.5 Dokumentace pro typ vozidla, který má být schválen, s popisem zmírňujících opatření, která byla provedena u systémů uvedených v seznamu, nebo typu vozidla a popisu způsobu, kterým řeší uvedená rizika: .....

9.6 Dokumentace pro typ vozidla, který má být schválen, s popisem ochrany vyhrazených prostředí pro ukládání a spouštění softwaru, služeb, aplikací nebo dat pocházejících z následného trhu: .....

9.7 Dokumentace pro typ vozidla, který má být schválen, popisující, jaké zkoušky byly použity k ověření kybernetické bezpečnosti typu vozidla a jeho systémů, a výsledek těchto zkoušek: .....

9.8 Popis zohlednění dodavatelského řetězce po stránce kybernetické bezpečnosti: .....

Příloha 1 – dodatek 1

Vzor prohlášení výrobce o shodě pro CSMS

Prohlášení výrobce o splnění požadavků na systém řízení kybernetické bezpečnosti

Název výrobce: .....

Adresa výrobce: .....

..... (*název výrobce*) potvrzuje, že jsou zavedeny postupy nezbytné ke splnění požadavků na systém řízení kybernetické bezpečnosti stanovených v bodě 7.2 předpisu OSN č. 155, a že tyto postupy budou nadále dodržovány. ....

Vystaveno v: ..... (*místo*)

Datum: .....

Jméno podepisující osoby: .....

Funkce podepisující osoby: .....

.....

(*razítko a podpis zástupce výrobce*)

PŘÍLOHA 2

Sdělení

(maximální formát: A4 (210 × 297 mm))

vydal: název správního orgánu:
.....
.....
.....

týkající se (2) Udělení schválení
Rozšíření schválení
Odejmutí schválení s účinkem ode dne dd/mm/rrrr
Odmítnutí schválení
Definitivního ukončení výroby

typu vozidla podle předpisu OSN č. 155

Schválení č.: .....

Rozšíření č.: .....

Důvod rozšíření: .....

1. Značka (obchodní název výrobce): .....

2. Typ a obecný obchodní popis (popisy) .....

3. Způsob označení typu, je-li na vozidle vyznačen: .....

3.1 Umístění tohoto označení: .....

4. Kategorie vozidla: .....

5. Jméno a adresa výrobce/zástupce výrobce: .....

6. Název (názvy) a adresa (adresy) výrobního závodu (závodů): .....

7. Číslo osvědčení o shodě pro systém řízení kybernetické bezpečnosti: .....

8. Technická zkušebna odpovědná za provádění zkoušek: .....

9. Datum vydání zkušebního protokolu: .....

10. Číslo zkušebního protokolu: .....

11. Připomínky: (jsou-li): .....

12. Místo: .....

13. Datum: .....

14. Podpis: .....

15. Je přiložen seznam informačních dokumentů uložených u schvalovacího orgánu, které lze obdržet na požádání:

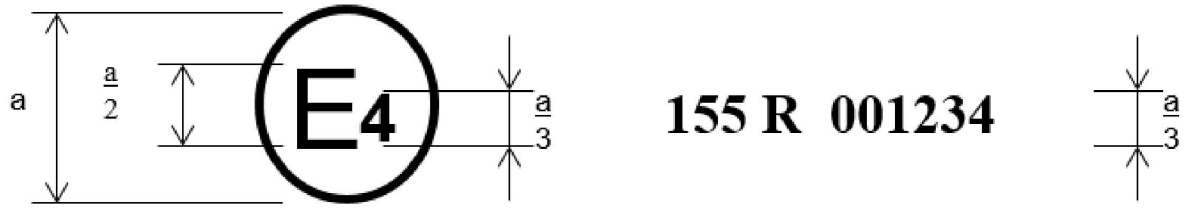
([1]) Rozlišovací číslo země, která schválení udělila / rozšířila / odmítla / odňala (viz ustanovení o schválení v předpise).
([2]) Nehodící se škrtněte.:

PŘÍLOHA 3

Uspořádání značky schválení typu

Vzor A

(viz bod 4.2 tohoto předpisu)



a = minimálně 8 mm

Výše uvedená značka schválení typu upevněná na vozidlo prokazuje, že typ silničního vozidla byl schválen v Nizozemsku (E4) v souladu s předpisem č. 155 pod číslem schválení 001234. První dvě číslice čísla schválení udávají, že schválení bylo uděleno v souladu s požadavky tohoto předpisu v jeho původním znění (00).

PŘÍLOHA 4

Vzor osvědčení o shodě pro systém řízení kybernetické bezpečnosti

Osvědčení o shodě pro systém řízení kybernetické bezpečnosti

v souladu s předpisem OSN č. 155

Číslo osvědčení [*referenční číslo*]

[……. *Schvalovací orgán*]

potvrzuje, že

Výrobce: ……

Adresa výrobce: ……

vyhovuje ustanovením bodu 7.2 předpisu č. 155

Ověření proběhlo dne: ……

(název a adresa schvalovacího orgánu nebo technické zkušebny): ……

Číslo protokolu: ……

Osvědčení je platné do [……*datum*]

V […… *místo*]

Dne [……*datum*]

[……*podpis*]

Přílohy: popis systému řízení kybernetické bezpečnosti výrobce

PŘÍLOHA 5

Seznam hrozeb a odpovídajících zmírňujících opatření

1. Tato příloha sestává ze tří částí: Část A této přílohy popisuje základní scénář hrozeb, zranitelnosti a metody útoku. Část B této přílohy popisuje zmírňující opatření pro hrozby, která jsou určena pro dané typy vozidel. Část C popisuje zmírňující opatření pro hrozby, která jsou určena pro oblasti mimo vozidla, např. na back-end IT infrastruktuře.

2. Část A, část B a část C se zohlední při posuzování a zmírňování rizik, která mají výrobci vozidel provádět.

3. V části A je uveden rejstřík obecného popisu zranitelností a jejich příslušných příkladů. Stejný rejstřík je uveden v tabulkách v částech B a C, aby každý útok/zranitelnost byly propojené se seznamem odpovídajících zmírňujících opatření.

4. Analýza hrozeb rovněž zohlední možné dopady útoku. Tyto dopady mohou pomoci zjistit závažnost rizika a určit další rizika. Možné dopady útoku mohou zahrnovat:

   a) negativní dopad na bezpečný provoz vozidla.

   b) přerušení provozu funkcí vozidla;

   c) úpravu softwaru vedoucí ke změně výkonu;

   d) úpravu softwaru bez účinku na provoz;

   e) narušení integrity dat;

   f) narušení důvěrnosti dat;

   g) narušení dostupnosti dat;

   h) jiné, včetně trestné činnosti.

Část A. Zranitelnost nebo metoda útoku v souvislosti s hrozbami

1. Obecné popisy hrozeb a souvisejících zranitelností nebo metod útoku jsou uvedeny v tabulce A1.

Tabulka A1

Část A. Seznam zranitelností nebo metod útoku v souvislosti s hrozbami

Obecné a specifičtější popisy zranitelnosti/hrozby			Příklad zranitelnosti nebo metody útoku	
4.3.1 Hrozby týkající se back-end serverů s dopadem na vozidla v provozu	1	Back-end servery použité k útoku na vozidlo nebo k extrakci dat	1.1	Zneužití oprávnění ze strany zaměstnanců (útok provedený zaměstnancem)
			1.2	Neoprávněný přístup k serveru z internetu (například prostřednictvím zadních vrátek (backdoor), neopravenými zranitelnostmi softwaru systému, útoky SQL nebo jinými prostředky)
			1.3	Neoprávněný fyzický přístup k serveru (například prostřednictvím USB média nebo připojením jiných médií k serveru)
	2	Narušení služeb back-end serveru s dopadem na provoz vozidla	2.1	Útok na back-end server zastaví jeho fungování, například tím, že zabrání interakci s vozidly a poskytování služeb, na které vozidla spoléhají

Obecné a specifičtější popisy zranitelnosti/hrozby			Příklad zranitelnosti nebo metody útoku	
	3	Ztráta nebo narušení údajů o vozidle uchovávaných na back-end serverech („narušení údajů“)	3.1	Zneužití oprávnění ze strany zaměstnanců (útok provedený zaměstnancem)
			3.2	Ztráta informací v cloudu. Citlivé údaje mohou být ztraceny v důsledku útoků nebo nehod, pokud jsou uloženy u externích poskytovatelů cloudových služeb.
			3.3	Neoprávněný přístup k serveru z internetu (například prostřednictvím zadních vrátek (backdoor), neopravenými zranitelnostmi softwaru systému, útoky SQL nebo jinými prostředky)
			3.4	Neoprávněný fyzický přístup k serveru (například prostřednictvím USB média nebo připojením jiných médií k serveru)
			3.5	Únik informací neúmyslným sdílením údajů (např. chyby ve správě systému)
4.3.2 Hrozby pro vozidla související s jejich komunikačními kanály	4	Zasílání podvržených zpráv nebo údajů přijímaných vozidlem (spoofing)	4.1	Zasílání podvržených zpráv vydáváním se za jinou osobu (např. u V2X komunikace využívající standard 802.11p při jízdě v konvoji, zpráv GNSS atd.)
			4.2	Útok typu „Sybil“ (podvrh, který simuluje existenci množství dalších vozidel na silnici)
	5	Komunikační kanály používané k provedení neoprávněné manipulace, výmazu nebo jiných změn kódu/údajů uchovávaných vozidlem	5.1	Komunikační kanály umožňují neoprávněné vložení kódu, například vložením upraveného binárního kódu do toku dat
			5.2	Komunikační kanály umožňují manipulaci s daty nebo s kódem v úložišti vozidla
			5.3	Komunikační kanály umožňují přepsání údajů nebo kódu v úložišti vozidla
			5.4	Komunikační kanály umožňují výmaz údajů nebo kódu v úložišti vozidla
			5.5	Komunikační kanály umožňují vložení údajů nebo dat do vozidla (zápis dat/kódu)
	6	Komunikační kanály umožňují přijetí nedůvěryhodných/ nespolehlivých zpráv nebo jsou zranitelné vůči útokům založeným na únosu relace/nebo opakování signálu	6.1	Přijímání informací z nespolehlivého nebo nedůvěryhodného zdroje
			6.2	Útok typu „man in the middle“/únos relace
			6.3	Útok opakováním signálu, například útok na komunikační bránu může umožnit útočníkovi nahrát neaktuální verzi softwaru řídicí jednotky motoru nebo firmwaru brány.

Obecné a specifičtější popisy zranitelnosti/hrozby			Příklad zranitelnosti nebo metody útoku	
	7	K informacím lze snadno získat přístup. Například odposlechem na komunikaci nebo umožněním neoprávněného přístupu k citlivým souborům nebo složkám	7.1	Zachycování informací / rušení signálu / monitorování komunikace
			7.2	Získání neoprávněného přístupu k souborům nebo údajům
	8	Útoky odepření služby prostřednictvím komunikačních kanálů s cílem narušit funkce vozidla	8.1	Zasílání velkého objemu zbytečných údajů do informačního systému vozidla, aby nebyl schopen poskytovat služby běžným způsobem
			8.2	Útok typu „black hole“, při kterém je útočník schopen blokovat zprávy mezi vozidly s cílem narušit komunikaci mezi nimi.
	9	Neoprávněný uživatel je schopen získat privilegovaný přístup k systémům vozidel.	9.1	Neoprávněný uživatel je schopen získat privilegovaný přístup, například k účtu správce.
	10	Viry mohou prostřednictvím komunikačního média infikovat systémy vozidla	10.1	Virus infikující systémy vozidla prostřednictvím komunikačních médií
	11	Zprávy přijaté vozidlem (např. X2V nebo diagnostické zprávy) nebo v něm přenášené obsahují škodlivý obsah	11.1	Škodlivé interní zprávy (např. síť řídicích jednotek CAN)
			11.2	Škodlivé zprávy V2X zprávy, např. zprávy zaslané vozidlu infrastrukturou nebo zprávy mezi vozidly (např. CAM, DENM)
			11.3	Škodlivé diagnostické zprávy
			11.4	Škodlivé proprietární zprávy (např. zprávy obvykle odesílané od výrobce původního zařízení nebo dodavatele součástí/systému/funkce)
4.3.3 Hrozby vůči vozidlům související s jejich postupy aktualizace	12	Zneužití nebo nesprávné použití postupů aktualizace	12.1	Zneužití postupů bezdrátové aktualizace softwaru. Do této kategorie spadá i podvržení aktualizace systému nebo firmwaru.
			12.2	Zneužití postupů aktualizace softwaru s využitím lokálního/fyzického připojení. Do této kategorie spadá i podvržení aktualizace systému nebo firmwaru.
			12.3	Se softwarem je před aktualizací manipulováno (čímž došlo k jeho poškození), ačkoli proces aktualizace nebyl narušen.

Obecné a specifičtější popisy zranitelnosti/hrozby			Příklad zranitelnosti nebo metody útoku	
			12.4	Zneužití kryptografických klíčů poskytovatele softwaru umožňující neplatnou aktualizaci
	13	Je možné odmítnout oprávněné aktualizace.	13.1	Útok odepření služby vůči aktualizačnímu serveru nebo síti, za účelem zabránit distribuci kritických aktualizací softwaru a/nebo odblokování funkcí určených pro konkrétní zákazníky
4.3.4 Hrozby pro vozidla související s nezamýšleným lidským jednáním umožňujícím kybernetický útok	15	Legitimní osoby jsou schopny provést kroky, kterými by neúmyslně umožnily kybernetický útok	15.1	Nevinná oběť (např. vlastník, provozovatel nebo pracovník údržby) může být zmanipulována k neúmyslnému nahrání škodlivého kódu nebo k umožnění útoku
			15.2	Nejsou dodržovány definované bezpečnostní postupy
4.3.5 Hrozby pro vozidla související s jejich vnější konektivitou a připojeními	16	Manipulace s konektivitou funkcí vozidla umožňuje kybernetický útok, toto se může týkat např. telematiky; systémů, které umožňují vzdálené ovládání; a systémů využívajících bezdrátové komunikace krátkého dosahu	16.1	Manipulace s funkcemi navrženými pro dálkové ovládání systémů, jako je vzdálený klíč, imobilizér a nabíjecí pilot
			16.2	Manipulace s telematickými systémy vozidel (např. s měřením teploty citlivého zboží, dálkové odemčení dveří nákladního prostoru)
			16.3	Rušení bezdrátových systémů s krátkým dosahem nebo senzorů
	17	Nahraný software třetí strany, např. zábavní aplikace, použitý jako prostředek k útoku na systémy vozidla	17.1	Poškozená aplikace nebo aplikace s nedostatečným zabezpečením softwaru použitá jako prostředek k útoku na systémy vozidla
	18	Zařízení připojená k vnějším rozhraním, např. pomocí portu USB nebo OBD, použitá jako prostředek k napadání systémů vozidel	18.1	Použití vnějších rozhraní, jako jsou porty USB nebo jiné porty, jako vektoru pro útok, například prostřednictvím vložení škodlivého kódu
			18.2	Připojení média infikovaného virem k systému vozidla
			18.3	Použití zařízení pro diagnostický přístup (např. zařízení připojených prostřednictvím portu OBD) k útoku, např. formou manipulace s parametry vozidla (přímo nebo nepřímo)
4.3.6 Ohrožení údajů/kódu vozidla	19	Extrakce údajů/kódu vozidla	19.1	Extrakce softwaru chráněného patentem nebo autorskými právy ze systémů vozidla (pirátství výrobků)
			19.2	Neoprávněný přístup k soukromým informacím o majiteli vozidla, jako je osobní identita, informace o platebním účtu, informace v adresáři, informace o poloze, elektronické identifikační číslo vozidla atd.
			19.3	Extrakce kryptografických klíčů

Obecné a specifičtější popisy zranitelnosti/hrozby			Příklad zranitelnosti nebo metody útoku	
	20	Manipulace s údaji/kódem vozidla	20.1	Nezákonné/nepovolené změny elektronického identifikačního čísla vozidla
			20.2	Zneužití totožnosti Například pokud uživatel chce při komunikaci se systémy mýtného nebo s back-end systémy výrobce zobrazovat jinou totožnost
			20.3	Opatření k obcházení monitorovacích systémů (např. hacking/tampering/ blokování zpráv, jako jsou údaje ODR, nebo počet jízd)
			20.4	Manipulace s daty za účelem podvržení údajů o řízení vozidla (např. počet ujetých kilometrů, rychlost jízdy, směry jízdy atd.)
			20.5	Neoprávněné změny systémových diagnostických údajů
	21	Výmaz údajů/kódu	21.1	Neoprávněné mazání nebo úprava údajů v systémovém protokolu událostí
	22	Instalace škodlivého kódu	22.2	Instalace nebo aktivace škodlivého kódu
	23	Instalace nového softwaru nebo přepis stávajícího softwaru	23.1	Falšování softwaru řídicího systému vozidla nebo informačního systému
	24	Narušení systémů nebo provozu	24.1	Útok odepření služby, ten lze na vnitřní síti vyvolat například zahlcením sběrnice řídicí jednotky CAN nebo vyvoláním závad na jednotce ECU prostřednictvím rychlého zasílání zpráv.
	25	Manipulace s parametry vozidla	25.1	Neoprávněný přístup umožňující podvržení parametrů konfigurace klíčových funkcí vozidla, jako jsou údaje o brzdách, prahová hodnota pro aktivaci airbagů atd.
			25.2	Neoprávněný přístup umožňující podvržení parametrů konfigurace, jako např. napájecí napětí a příkon, teplota baterie atd.
4.3.7 Potenciální zranitelnosti, které by mohly být zneužity, pokud by nebyla dostatečně chráněna nebo zabezpečena	26	Šifrovací technologie mohou být ohroženy nebo nejsou správně použity	26.1	Kombinace krátkých šifrovacích klíčů a dlouhé doby platnosti umožňuje útočníkovi prolomit šifrování
			26.2	Nedostatečné používání šifrovacích algoritmů k ochraně citlivých systémů
			26.3	Používání zastaralých kryptografických algoritmů, jejichž použitelnost brzy skončí nebo již skončila

Obecné a specifičtější popisy zranitelnosti/hrozby			Příklad zranitelnosti nebo metody útoku	
	27	Části nebo materiál by mohly být zneužity k umožnění útoku na vozidla	27.1	Hardware nebo software, který je navržen tak, aby umožnil útok, nebo který nesplňuje konstrukční kritéria pro zastavení útoku
	28	Vývoj softwaru nebo hardwaru umožňuje výskyt zranitelností	28.1	Chyby v softwaru Chyby v softwaru mohou poskytnout základ pro zneužitelné zranitelnosti. To platí zejména v případě, že software nebyl testován, aby se ověřilo, že kód neobsahuje známé chyby, a snížilo se riziko výskytu neznámých chyb v kódu.
			28.2	Využití pozůstatků z vývoje (např. portů pro ladění, JTAG portů, mikroprocesorů, vývojářských certifikátů, přístupových hesel atd.) může umožnit přístup k jednotce ECU nebo umožnit útočníkům získat přístup s vyššími oprávněními
	29	Zranitelnosti způsobené koncepcí sítě	29.1	Zbytečně vysoký počet portů otevřených vůči Internetu umožňujících přístup k síťovým systémům
			29.2	Obcházení oddělení sítí za účelem získání kontroly. Konkrétním příkladem je využití nechráněných síťových bran nebo přístupových bodů (jako jsou brány mezi nákladním vozidlem a přívěsem) k obejití ochrany a získání přístupu k jiným síťovým segmentům za účelem provádění škodlivých kroků, jako je zasílání libovolných zpráv sběrnici CAN.
	31	Je možný neúmyslný přenos údajů	31.1	Únik informací K úniku osobních údajů může dojít při změně uživatele automobilu (např. v případě prodeje nebo pronájmu vozidla).
	32	Fyzická manipulace se systémy může umožnit útok	32.1	Manipulace s elektronickým hardwarovým vybavením, např. přidáním neautorizovaného elektronického hardwarového vybavení do vozidla s cílem umožnit útok typu „man-in-the-middle“ Nahrazení autorizovaného elektronického hardwaru (např. senzorů) neautorizovaným elektronickým hardwarem Manipulace s informacemi zaznamenanými senzorem (například použitím magnetu k nedovolené manipulaci s Hall efektovým senzorem, který je připojen k převodovce)

Část B. Zmírňující opatření pro hrozby zaměřené na vozidla

1. Zmírňující opatření pro komunikační kanály vozidla

Zmírňující opatření pro hrozby související s komunikačními kanály vozidel jsou uvedena v tabulce B1.

Tabulka B1

Zmírňující opatření pro hrozby související s komunikačními kanály vozidel

Odkaz na tabulku-A1	Hrozby pro „komunikační kanály vozidla“	Odkaz	Zmírňující opatření
4.1	Zasílání podvržených zpráv (např. u V2X komunikace využívající standard 802.11p při jízdě v konvoji, zpráv GNSS atd.) vydáváním se za jinou osobu	M10	Vozidlo ověří pravost a neporušenost zpráv, které obdrží
4.2	Útok typu „Sybil“ (podvrh, který simuluje existenci množství dalších vozidel na silnici)	M11	Pro ukládání kryptografických klíčů musí být zavedeny bezpečnostní mechanismy (např. používání hardwarových bezpečnostních modulů)
5.1	Komunikační kanály umožňují neoprávněné vložení kódu do úložiště vozidla, například vložením upraveného binárního kódu do toku dat	M10 M6	Vozidlo ověří pravost a neporušenost zpráv, které obdrží Aby se minimalizovala rizika, musí systémy zahrnovat bezpečnost již od návrhu
5.2	Komunikační kanály umožňují manipulaci s údaji nebo s kódem v úložišti vozidla	M7	K ochraně systémových údajů/kódu se použijí techniky a koncepce řízení přístupu
5.3	Komunikační kanály umožňují přepsání dat nebo kódu v úložišti vozidla		
5.4 21.1	Komunikační kanály umožňují výmaz dat nebo kódu v úložišti vozidla		
5.5	Komunikační kanály umožňují vložení dat nebo kódu do systémů vozidla (zápis dat/kódu)		
6.1	Přijímání informací z nespolehlivého nebo nedůvěryhodného zdroje	M10	Vozidlo ověří pravost a neporušenost zpráv, které obdrží
6.2	Útok typu „man in the middle“/únos relace	M10	Vozidlo ověří pravost a neporušenost zpráv, které obdrží
6.3	Útok opakováním signálu, například útok na komunikační bránu může umožnit útočníkovi nahrát neaktuální verzi softwaru řídicí jednotky motoru nebo firmwaru brány.		
7.1	Zachycování informací / rušení signálu / monitorování komunikace	M12	Důvěrné údaje zasílané do vozidla nebo z vozidla jsou chráněny
7.2	Získání neoprávněného přístupu k souborům nebo datům	M8	Díky návrhu systému a řízení přístupu by neoprávněné osoby neměly mít možnost získat přístup k osobním údajům nebo kritickým systémovým údajům. Příklad mechanismů zabezpečení lze nalézt v OWASP

Odkaz na tabulku-A1	Hrozby pro „komunikační kanály vozidla“	Odkaz	Zmírňující opatření
8.1	Zasílání velkého objemu zbytečných dat do informačního systému vozidla, aby nebyl schopen poskytovat služby běžným způsobem	M13	Použijí se opatření k odhalování útoku odepření služby a zotavení se z takového útoku
8.2	Útok typu „black hole“, přerušení komunikace mezi vozidly blokováním přenosu zpráv do jiných vozidel	M13	Použijí se opatření k odhalování útoku odepření služby a zotavení se z takového útoku
9.1	Neoprávněný uživatel je schopen získat privilegovaný přístup, například k účtu správce	M9	Použijí se opatření pro předcházení neoprávněnému přístupu a pro jeho odhalování
10.1	Virus infikující systémy vozidla prostřednictvím komunikačních médií	M14	Měla by být zvážena opatření na ochranu systémů proti virům/malwaru
11.1	Škodlivé interní zprávy (např. zprávy CAN)	M15	Měla by být zvážena opatření k odhalení škodlivých interních zpráv nebo procesů
11.2	Škodlivé zprávy V2X zprávy, např. zprávy zaslané vozidlu infrastrukturou nebo zprávy mezi vozidly (např. CAM, DENM)	M10	Vozidlo ověří pravost a neporušenost zpráv, které obdrží
11.3	Škodlivé diagnostické zprávy		
11.4	Škodlivé proprietární zprávy (např. zprávy obvykle odesílané od výrobce původního zařízení nebo dodavatele součástí/systému/funkce)		

2. Zmírňující opatření pro proces aktualizace

Zmírňující opatření pro hrozby související s procesem aktualizace jsou uvedena v tabulce B2.

Tabulka B2

Zmírňující opatření pro hrozby související s procesem aktualizace

Odkaz na tabulku-A1	Hrozby pro proces aktualizace	Odkaz	Zmírňující opatření
12.1	Zneužití postupů bezdrátové aktualizace softwaru. Do této kategorie spadá i podvržení aktualizace systému nebo firmwaru.	M16	Použijí se postupy pro zabezpečenou aktualizaci softwaru
12.2	Zneužití postupů aktualizace softwaru s využitím lokálního/fyzického připojení. Do této kategorie spadá i podvržení aktualizace systému nebo firmwaru.		
12.3	Se softwarem je před aktualizací manipulováno (čímž došlo k jeho poškození), ačkoli proces aktualizace nebyl narušen.		

Odkaz na tabulku-A1	Hrozby pro proces aktualizace	Odkaz	Zmírňující opatření
12.4	Zneužití kryptografických klíčů poskytovatele softwaru umožňující neplatnou aktualizaci	M11	Pro ukládání kryptografických klíčů musí být zavedeny mechanismy zabezpečení.
13.1	Útok odepření služby vůči aktualizačnímu serveru nebo síti, za účelem zabránit distribuci kritických aktualizací softwaru a/nebo odblokování funkcí určených pro konkrétní zákazníky	M3	Musí být zavedeny mechanismy zabezpečení back-end systémů. Pro back-end servery, které jsou kriticky důležité pro poskytování služeb, existují opatření na obnovu v případě výpadku systému. Příklad mechanismů zabezpečení lze nalézt v OWASP

3. Zmírňující opatření pro nezamýšlené lidské jednání umožňující kybernetický útok

Zmírňující opatření pro hrozby související s nezamýšleným lidským jednáním umožňujícím kybernetický útok jsou uvedena v tabulce B3.

Tabulka B3

Zmírňující opatření pro hrozby související s nezamýšleným lidským jednáním umožňujícím kybernetický útok

Odkaz na tabulku-A1	Hrozby související s nezamýšleným lidským jednáním	Odkaz	Zmírňující opatření
15.1	Nevinná oběť (např. vlastník, provozovatel nebo pracovník údržby) může být zmanipulována k neúmyslnému nahrání škodlivého kódu nebo k umožnění útoku	M18	Budou zavedena opatření pro definování a řízení uživatelských rolí a přístupových práv na základě zásady nejnižších možných oprávnění.
15.2	Nejsou dodržovány definované bezpečnostní postupy	M19	Organizace zajistí, aby bezpečnostní postupy byly definovány a dodržovány, včetně zaznamenávání činností a přístupů v souvislosti s řízením bezpečnostních funkcí.

4. Zmírňující opatření pro hrozby související s vnější konektivitou a připojeními

Zmírňující opatření pro hrozby související s vnější konektivitou a připojeními jsou uvedena v tabulce B4.

Tabulka B4

Zmírňující opatření pro hrozby související s vnější konektivitou a připojeními

Odkaz na tabulkuA1	Hrozby pro vnější konektivitu a připojení	Odkaz	Zmírňující opatření
16.1	Manipulace s funkcemi navrženými pro dálkové ovládání systémů, jako je vzdálený klíč, imobilizér a nabíjecí pilot	M20	Pro systémy s dálkovým přístupem musí být zavedeny mechanismy zabezpečení.
16.2	Manipulace s telematickými systémy vozidel (např. s měřením teploty citlivého zboží, dálkové odemčení dveří nákladního prostoru)		

Odkaz na tabulku A1	Hrozby pro vnější konektivitu a připojení	Odkaz	Zmírňující opatření
16.3	Rušení bezdrátových systémů s krátkým dosahem nebo senzorů		
17.1	Poškozená aplikace nebo aplikace s nedostatečným zabezpečením softwaru použitá jako prostředek k útoku na systémy vozidla	M21	Software musí být posouzen z hlediska bezpečnosti, ověřen a jeho integrita musí být chráněna. Musí být zavedeny bezpečnostní mechanismy, které minimalizují riziko, které představuje software třetí strany, který je určen pro instalaci ve vozidle, nebo jehož instalaci lze očekávat
18.1	Použití vnějších rozhraní, jako jsou porty USB nebo jiné porty, jako vektoru pro útok, například prostřednictvím vložení škodlivého kódu	M22	Musí být zavedeny mechanismy zabezpečení vnějších rozhraní
18.2	Připojení média infikovaného virem k systému vozidla		
18.3	Použití zařízení pro diagnostický přístup (např. zařízení připojených prostřednictvím portu OBD) k útoku, např. formou manipulace s parametry vozidla (přímo nebo nepřímo)	M22	Musí být zavedeny mechanismy zabezpečení vnějších rozhraní

5. Zmírňující opatření pro potenciální cíle útoků nebo motivace pro útok

Zmírňující opatření pro hrozby související s potenciálními cíli útoků a motivy pro útok jsou uvedena v tabulce B5.

Tabulka B5

Zmírňující opatření pro hrozby související s potenciálními cíli útoků a motivy pro útok

Odkaz na tabulku A1	Hrozby pro potenciální cíle útoků a motivy pro útok	Odkaz	Zmírňující opatření
19.1	Extrakce softwaru chráněného patentem nebo autorskými právy ze systémů vozidla (pirátství výrobků / odcizení softwaru)	M7	K ochraně systémových dat/kódu se použijí techniky a koncepce řízení přístupu Příklad mechanismů zabezpečení lze nalézt v OWASP
19.2	Neoprávněný přístup k soukromým informacím o majiteli vozidla, jako je osobní identita, informace o platebním účtu, informace v adresáři, informace o poloze, elektronické identifikační číslo vozidla atd.	M8	Díky návrhu systému a řízení přístupu by neoprávněné osoby neměly mít možnost získat přístup k osobním údajům nebo kritickým systémovým údajům. Příklad mechanismů zabezpečení lze nalézt v OWASP
19.3	Extrakce kryptografických klíčů	M11	Pro ukládání kryptografických klíčů musí být zavedeny bezpečnostní mechanismy, např. používání bezpečnostních modulů
20.1	Nezákonné/nepovolené změny elektronického identifikačního čísla vozidla	M7	K ochraně systémových dat/kódu se použijí techniky a koncepce řízení přístupu Příklad mechanismů zabezpečení lze nalézt v OWASP
20.2	Zneužití totožnosti Například pokud uživatel chce při komunikaci se systémy mýtného nebo s back-end systémy výrobce zobrazovat jinou totožnost		
20.3	Opatření k obcházení monitorovacích systémů (např. hacking/tampering/ blokování zpráv, jako jsou údaje ODR, nebo počet jízd)	M7	K ochraně systémových dat/kódu se použijí techniky a koncepce řízení přístupu Příklad mechanismů zabezpečení lze nalézt v OWASP

Odkaz na tabulkuA1	Hrozby pro potenciální cíle útoků a motivy pro útok	Odkaz	Zmírňující opatření
20.4	Manipulace s daty za účelem podvržení údajů o řízení vozidla (např. počet ujetých kilometrů, rychlost jízdy, směry jízdy atd.)		Útoky formou manipulace s daty ze senzorů nebo s přenášenými daty by mohly být zmírněny porovnáváním údajů z různých zdrojů informací
20.5	Neoprávněné změny systémových diagnostických údajů		
21.1	Neoprávněné mazání nebo úprava údajů v systémovém protokolu událostí	M7	K ochraně systémových dat/kódu se použijí techniky a koncepce řízení přístupu Příklad mechanismů zabezpečení lze nalézt v OWASP
22.2	Instalace nebo aktivace škodlivého kódu	M7	K ochraně systémových dat/kódu se použijí techniky a koncepce řízení přístupu Příklad mechanismů zabezpečení lze nalézt v OWASP
23.1	Falšování softwaru řídicího systému vozidla nebo informačního systému		
24.1	Útok odepření služby, ten lze na vnitřní síti vyvolat například zahlcením sběrnice řídicí jednotky CAN nebo vyvoláním závad na jednotce ECU prostřednictvím rychlého zasílání zpráv.	M13	Použijí se opatření k odhalování útoku odepření služby a zotavení se z takového útoku
25.1	Neoprávněný přístup umožňující podvržení parametrů konfigurace klíčových funkcí vozidla, jako jsou údaje o brzdách, prahová hodnota pro aktivaci airbagů atd.	M7	K ochraně systémových dat/kódu se použijí techniky a koncepce řízení přístupu Příklad mechanismů zabezpečení lze nalézt v OWASP
25.2	Neoprávněný přístup umožňující podvržení parametrů konfigurace, jako např. napájecí napětí a příkon, teplota baterie atd.		

6. Zmírňující opatření pro potenciální zranitelnosti, které by mohly být zneužity, pokud by nebyly dostatečně chráněny nebo zabezpečeny

Zmírňující opatření pro hrozby související s potenciálními zranitelnostmi, které by mohly být zneužity, pokud by nebyly dostatečně chráněny nebo zabezpečeny, jsou uvedena v tabulce B6.

Tabulka B6

Zmírňující opatření pro hrozby související s potenciálními zranitelnostmi, které by mohly být zneužity, pokud by nebyly dostatečně chráněny nebo zabezpečeny

Odkaz na tabulku-A1	Hrozby související s potenciálními zranitelnostmi, které by mohly být zneužity, pokud by nebyly dostatečně chráněny nebo zabezpečeny	Odkaz	Zmírňující opatření
26.1	Kombinace krátkých šifrovacích klíčů a dlouhé doby platnosti umožňuje útočníkovi prolomit šifrování	M23	Musí být dodržovány osvědčené postupy kybernetické bezpečnosti v oblasti vývoje softwaru a hardwaru

Odkaz na tabulku-A1	Hrozby související s potenciálními zranitelnostmi, které by mohly být zneužity, pokud by nebyly dostatečně chráněny nebo zabezpečeny	Odkaz	Zmírňující opatření
26.2	Nedostatečné používání šifrovacích algoritmů k ochraně citlivých systémů		
26.3	Používání zastaralých šifrovacích algoritmů		
27.1	Hardware nebo software, který je navržen tak, aby umožnil útok, nebo který nesplňuje konstrukční kritéria pro zastavení útoku	M23	Musí být dodržovány osvědčené postupy kybernetické bezpečnosti v oblasti vývoje softwaru a hardwaru
28.1	Chyby v softwaru mohou poskytnout základ pro zneužitelné zranitelnosti. To platí zejména v případě, že software nebyl testován, aby se ověřilo, že kód neobsahuje známé chyby, a snížilo se riziko výskytu neznámých chyb v kódu.	M23	Musí být dodržovány osvědčené postupy kybernetické bezpečnosti v oblasti vývoje softwaru a hardwaru. Testování kybernetické bezpečnosti s odpovídajícím pokrytím hrozeb
28.2	Využití pozůstatků z vývoje (např. portů pro ladění, JTAG portů, mikroprocesorů, vývojářských certifikátů, přístupových hesel atd.) může útočníkovi umožnit přístup k jednotce ECU nebo získat přístup s vyššími oprávněními		
29.1	Zbytečně vysoký počet portů otevřených vůči Internetu umožňujících přístup k síťovým systémům		
29.2	Obcházení oddělení sítí za účelem získání kontroly Konkrétním příkladem je využití nechráněných síťových bran nebo přístupových bodů (jako jsou brány mezi nákladním vozidlem a přívěsem) k obejití ochrany a získání přístupu k jiným síťovým segmentům za účelem provádění škodlivých kroků, jako je zasílání libovolných zpráv sběrnici CAN.	M23	Musí být dodržovány osvědčené postupy kybernetické bezpečnosti v oblasti vývoje softwaru a hardwaru. Musí být dodržovány osvědčené postupy kybernetické bezpečnosti v oblastech návrhu systému a systémové integrace

7. Zmírňující opatření pro ztrátu nebo únik dat z vozidla

Zmírňující opatření pro hrozby související s možností ztráty nebo úniku dat z vozidla jsou uvedena v tabulce B7.

Tabulka B7

Zmírňující opatření pro hrozby související s možností ztráty nebo úniku dat z vozidla

Odkaz na tabulku-A1	Hrozby související s možností ztráty nebo úniku dat z vozidla	Odkaz	Zmírňující opatření
31.1	Únik informací K úniku osobních údajů může dojít při změně uživatele automobilu (např. v případě prodeje nebo pronájmu vozidla).	M24	Uchovávání osobních údajů se řídí osvědčenými postupy pro ochranu integrity a důvěrnosti údajů.

8. Zmírňující opatření proti fyzické manipulaci se systémy za účelem umožnění útoku

Zmírňující opatření pro hrozby související s fyzickou manipulací se systémy za účelem umožnění útoku jsou uvedena v tabulce B8.

Tabulka B8

Zmírňující opatření pro hrozby související s fyzickou manipulací se systémy za účelem umožnění útoku

Odkaz na tabulku-A1	Hrozba fyzické manipulace se systémy za účelem umožnění útoku	Odkaz	Zmírňující opatření
32.1	Manipulace s OEM hardwarovým vybavením, např. přidáním neautorizovaného hardwarového vybavení do vozidla s cílem umožnit útok typu „man-in-the-middle“	M9	Použijí se opatření pro předcházení neoprávněnému přístupu a pro jeho odhalování

Část C. Zmírňující opatření pro hrozby zaměřené na oblasti vozidla

1. Zmírňující opatření pro back-end servery

Zmírňující opatření pro hrozby související s back-end servery jsou uvedena v tabulce C1.

Tabulka C1

Zmírňující opatření pro hrozby související s back-end servery

Odkaz na tabulku-A1	Hrozby pro back-end servery	Odkaz	Zmírňující opatření
1.1 & 3.1	Zneužití oprávnění ze strany zaměstnanců (útok provedený zaměstnancem)	M1	Back-end systémy musí být chráněny bezpečnostními mechanismy minimalizujícími riziko útoku provedeného zaměstnanci
1.2 & 3.3	Neoprávněný přístup k serveru z internetu (například prostřednictvím zadních vrátek (backdoor), neopravenými zranitelnostmi softwaru systému, útoky SQL nebo jinými prostředky)	M2	Back-end systémy musí být chráněny bezpečnostními mechanismy minimalizujícími riziko neoprávněného přístupu Příklad mechanismů zabezpečení lze nalézt v OWASP
1.3 & 3.4	Neoprávněný fyzický přístup k serveru (například prostřednictvím USB média nebo připojením jiných médií k serveru)	M8	Díky návrhu systému a řízení přístupu by neoprávněné osoby neměly mít možnost získat přístup k osobním údajům nebo kritickým systémovým údajům.
2.1	Útok na back-end server zastaví jeho fungování, například tím, že zabrání interakci s vozidly a poskytování služeb, na které vozidla spoléhají	M3	Musí být zavedeny mechanismy zabezpečení back-end systémů. Pro back-end servery, které jsou kriticky důležité pro poskytování služeb, existují opatření na obnovu v případě výpadku systému. Příklad mechanismů zabezpečení lze nalézt v OWASP
3.2	Ztráta informací v cloudu. Citlivé údaje mohou být ztraceny v důsledku útoků nebo nehod, pokud jsou uloženy u externích poskytovatelů cloudových služeb.	M4	Musí být zavedeny mechanismy zabezpečení s cílem minimalizovat rizika spojená s cloudovými službami. Příklady mechanismů zabezpečení lze nalézt v pokynech pro cloud computing projektu OWASP a strategie NCSC.
3.5	Únik informací neúmyslným sdílením údajů (např. chyby ve správě systému, ukládání dat na serverech servisů)	M5	Back-end systémy musí být chráněny bezpečnostními mechanismy minimalizujícími riziko úniku dat Příklad mechanismů zabezpečení lze nalézt v OWASP

2. Zmírňující opatření pro nezamýšlené lidské jednání

Zmírňující opatření pro hrozby související s nezamýšleným lidským jednáním jsou uvedena v tabulce C2.

Tabulka C2

Zmírňující opatření pro hrozby související s nezamýšleným lidským jednáním

Odkaz na tabulku-A1	Hrozby související s nezamýšleným lidským jednáním	Odkaz	Zmírňující opatření
15.1	Nevinná oběť (např. vlastník, provozovatel nebo pracovník údržby) může být zmanipulována k neúmyslnému nahrání škodlivého kódu nebo k umožnění útoku	M18	Budou zavedena opatření pro definování a řízení uživatelských rolí a přístupových práv na základě zásady nejnižších možných oprávnění.
15.2	Nejsou dodržovány definované bezpečnostní postupy	M19	Organizace zajistí, aby bezpečnostní postupy byly definovány a dodržovány, včetně zaznamenávání činností a přístupů v souvislosti s řízením bezpečnostních funkcí.

3. Zmírňující opatření pro hrozbu fyzické ztráty dat

Zmírňující opatření pro hrozby související s hrozbou fyzické ztráty dat jsou uvedena v tabulce C3.

Tabulka C3

Zmírňující opatření pro hrozby související s hrozbou fyzické ztráty dat

Odkaz na tabulku-A1	Hrozba fyzické ztráty dat	Odkaz	Zmírňující opatření
30.1	Škody způsobené třetí stranou. Citlivá data mohou být ztracena nebo poškozena v důsledku fyzických škod při dopravní nehodě nebo v případě krádeže.	M24	Uchovávání osobních údajů se řídí osvědčenými postupy pro ochranu integrity a důvěrnosti údajů. Příklady mechanismů zabezpečení lze nalézt v ISO/SC27/WG5
30.2	Ztráta dat v důsledku konfliktu DRM (správy digitálních práv) Uživatelská data mohou být vymazána v důsledku problémů v systému DRM.		
30.3	Může dojít ke ztrátě nebo poškození citlivých dat v důsledku opotřebení IT součástí, což může způsobit navazující problémy (například v případě změny klíče).		