2025/5

10.1.2025

Kun de originale FN/ECE-tekster har retlig virkning i henhold til folkeretten. Dette regulativs nuværende status og ikrafttrædelsesdato bør kontrolleres i den seneste version af FN/ECE's statusdokument TRANS/WP.29/343, der findes på adressen: https://unece.org/status-1958-agreement-and-annexed-regulations

FN-regulativ nr. 155 - Ensartede forskrifter for godkendelse af køretøjer for så vidt angår cybersikkerhed og systemer til forvaltning af cybersikkerhed [2025/5]

Omfattende al gældende tekst frem til:

Supplement 3 til den oprindelige udgave af regulativet – ikrafttrædelsesdato: 10. januar 2025

Dette dokument tjener udelukkende som dokumentationsredskab. De autentiske og juridisk bindende tekster er:

— ECE/TRANS/WP.29/2020/79 (som ændret ved ECE/TRANS/WP.29/2020/94 og ECE/TRANS/WP.29/2020/97)

— ECE/TRANS/WP.29/2022/54

— ECE/TRANS/WP.29/2023/70 og

— ECE/TRANS/WP.29/2024/55

INDHOLDSFORTEGNELSE

Regulativ

1. Anvendelsesområde
2. Definitioner
3. Ansøgning om godkendelse
4. Mærkning
5. Godkendelse
6. Overensstemmelsescertifikat for systemet til forvaltning af cybersikkerhed
7. Specifikationer
8. Ændring af køretøjstypen og udvidelse af typegodkendelsen
9. Produktionens overensstemmelse
10. Sanktioner i tilfælde af produktionens manglende overensstemmelse
11. Endeligt ophør af produktionen
12. Navne og adresser på tekniske tjenester, som er ansvarlige for udførelse af godkendelsesprøvning, og på de typegodkendende myndigheder

Bilag

1 Oplysningsskema

2 Meddelelse

3 Godkendelsesmærkets udformning

4 Model for CSMS-overensstemmelsescertifikatet

5 Liste over trusler og tilknyttede modforanstaltninger

1. Anvendelsesområde

1.1. Regulativet finder anvendelse på køretøjer for så vidt angår cybersikkerhed i klasse L, M, N og O, hvis de er udstyret med mindst én elektronisk kontrolenhed.

1.2. Dette regulativ berører ikke andre FN-regulativer, regionale bestemmelser eller national lovgivning om adgang for autoriserede tredjeparter til køretøjet, dets data, funktioner og ressourcer samt betingelserne for en sådan adgang. Det berører heller ikke anvendelsen af national og regional lovgivning om privatlivets fred og beskyttelse af fysiske personer i forbindelse med behandling af deres personoplysninger.

1.3. Dette regulativ berører ikke andre FN-regulativer, regionale bestemmelser eller national lovgivning om udvikling og montering/systemintegration af reservedele og fysiske og digitale komponenter i forbindelse med cybersikkerhed.

2. Definitioner

I dette regulativ forstås ved:

2.1. "køretøjstype": køretøjer, der som minimum ikke udviser forskelle på følgende væsentlige punkter:

a) fabrikantens betegnelse for køretøjstypen

b) væsentlige aspekter af den elektriske/elektroniske arkitektur og eksterne grænseflader for så vidt angår cybersikkerhed

2.2. "cybersikkerhed": den tilstand, i hvilken køretøjer benyttet til vejkørsel og deres funktioner er beskyttet mod cybertrusler mod elektriske eller elektroniske komponenter

2.3. "system til forvaltning af cybersikkerhed (CSMS)": en systematisk, risikobaseret tilgang, der definerer organisatoriske processer, ansvarsområder og forvaltning med henblik på at håndtere risici i forbindelse med cybertrusler mod køretøjer og beskytte dem mod cyberangreb

2.4. "system": et sæt af komponenter og/eller delsystemer, der implementerer en eller flere funktioner

2.5. "udviklingsfasen": perioden inden typegodkendelsen af køretøjstypen

2.6. "produktionsfasen": den tid, det tager at producere en køretøjstype

2.7. "efterproduktionsfasen": den periode, der ligger mellem det tidspunkt, hvor en køretøjstype ikke længere produceres, og indtil alle køretøjer i køretøjstypen er udrangeret. Køretøjer med en specifik køretøjstype vil være i drift i denne fase, men vil ikke længere blive fremstillet. Fasen ophører, når der ikke længere er nogen køretøjer af den specifikke køretøjstype i drift

2.8. "modforanstaltning": en risikoreducerende foranstaltning

2.9. "risiko": det potentiale, en given trussel har til at udnytte sårbarheder i et køretøj og derved skade organisationen eller en enkeltperson

2.10. "risikovurdering": den overordnede proces med at konstatere, anerkende og beskrive risici (risikoidentifikation), forstå risikoens art og bestemme risikoniveauet (risikoanalyse), og sammenligne resultaterne af risikoanalysen med risikokriterier for at afgøre, om risikoen og/eller dens omfang er acceptabel eller tålelig (risikoevaluering)

2.11. "risikostyring": koordinerede aktiviteter til at lede og kontrollere en organisation med hensyn til risiko

2.12. "trussel": en potentiel årsag til en uønsket hændelse, der kan føre til skade på et system, en organisation eller en enkeltperson

2.13. "sårbarhed": en svaghed i et aktiv eller en modforanstaltning, som kan udnyttes af en eller flere trusler.

3. Ansøgning om godkendelse

3.1. Ansøgning om godkendelse af en køretøjstype for så vidt angår cybersikkerhed indgives af køretøjsfabrikanten eller dennes bemyndigede repræsentant.

3.2. Ansøgningen skal bilægges nedennævnte dokumenter i tre eksemplarer og følgende oplysninger:

3.2.1. En beskrivelse af køretøjstypen for så vidt angår punkterne specificeret i bilag 1 til dette regulativ.

3.2.2. Hvis det påvises, at oplysninger er omfattet af intellektuelle ejendomsrettigheder eller er en del af fabrikantens eller dennes leverandørers specifikke knowhow, stiller fabrikanten eller dennes leverandører tilstrækkelige oplysninger til rådighed med henblik på at gøre det muligt at udføre kontrollerne i dette regulativ på behørig vis. Sådanne oplysninger behandles fortroligt.

3.2.3. Overensstemmelsescertifikatet for systemet til forvaltning af cybersikkerhed i henhold til punkt 6 i dette regulativ.

3.3. Dokumentationen skal foreligge i to dele:

a) Den formelle dokumentationspakke, der kræves med henblik på godkendelse, vedlagt materialet nævnt i bilag 1, skal leveres til den godkendende myndighed eller dens tekniske tjeneste på tidspunktet for indgivelse af ansøgningen om typegodkendelse. Denne dokumentationspakke skal af den godkendende myndighed eller dens tekniske tjeneste anvendes som referenceramme for godkendelsesprocessen. Den godkendende myndighed eller dens tekniske tjeneste skal sørge for, at denne dokumentationspakke er tilgængelig i mindst 10 år, regnet fra tidspunktet for det endelige ophør af produktionen af køretøjstypen.

b) Yderligere materiale, der er relevant for kravene i dette regulativ, kan opbevares af fabrikanten, men skal stilles til rådighed for gennemgang på godkendelsestidspunktet. Fabrikanten skal sørge for, at alle oplysninger, der er til rådighed for inspektion på tidspunktet for typegodkendelsen, fortsat er tilgængelige i mindst 10 år regnet fra tidspunktet for det endelige ophør af produktionen af køretøjstypen.

4. Mærkning

4.1. Ethvert køretøj, som er i overensstemmelse med en type, som er godkendt efter dette regulativ, skal på et let synligt og let tilgængeligt sted, der er angivet i godkendelsesattesten, være påført et internationalt godkendelsesmærke bestående af følgende:

4.1.1. en cirkel, som omslutter bogstavet "E" efterfulgt af kendingsnummeret på den stat, som har meddelt godkendelse

4.1.2. nummeret på dette regulativ efterfulgt af bogstavet "R", en bindestreg og godkendelsesnummeret til højre for den cirkel, der er foreskrevet i punkt 4.1.1 ovenfor.

4.2. Er køretøjet i overensstemmelse med en køretøjstype, som i henhold til et eller flere andre af de til overenskomsten vedføjede regulativer er godkendt i samme stat, som har meddelt godkendelse efter dette regulativ, behøver det i punkt 4.1.1. ovenfor foreskrevne symbol ikke gentages. I så fald skal numrene på regulativet og godkendelserne samt de ekstra symboler for alle regulativer, i henhold til hvilke der er meddelt godkendelse i det land, hvor godkendelsen er meddelt i henhold til dette regulativ, placeres i lodrette kolonner til højre for det symbol, der er beskrevet i punkt 4.1.1 ovenfor.

4.3. Godkendelsesmærket skal være let læseligt og må ikke kunne slettes.

4.4. Godkendelsesmærket skal anbringes på eller tæt ved den mærkeplade, fabrikanten har anbragt på køretøjet.

4.5. Bilag 3 til dette regulativ indeholder eksempler på godkendelsesmærkets udformning.

5. Godkendelse

5.1. De godkendende myndigheder meddeler kun typegodkendelse for så vidt angår cybersikkerhed for køretøjstyper, som opfylder kravene i dette regulativ.

5.1.1. Den godkendende myndighed eller den tekniske tjeneste skal ved hjælp af dokumentkontrol efterprøve, at køretøjsfabrikanten har truffet de foranstaltninger for køretøjstypen, der er nødvendige for:

a) gennem forsyningskæden at indhente og kontrollere de oplysninger, der kræves i henhold til dette regulativ, så det kan påvises, at leverandør-relaterede risici identificeres og håndteres

b) at dokumentere risikovurderinger (udført under udviklingsfasen eller med tilbagevirkende kraft), prøvningsresultater og modforanstaltninger anvendt på køretøjstypen, herunder konstruktionsoplysninger til støtte for risikovurderingen

c) at implementere passende cybersikkerhedsforanstaltninger i konstruktionen af køretøjstypen

d) at detektere og håndtere eventuelle cybersikkerhedsangreb

e) at logge data til støtte for detektering af cyberangreb og sikre en IT-kriminalteknisk kapacitet, der gør det muligt at analysere forsøg på cyberangreb eller gennemførte cyberangreb.

5.1.2. Den godkendende myndighed eller den tekniske tjeneste skal ved prøvning af et køretøj af den relevante køretøjstype kontrollere, at køretøjsfabrikanten har implementeret de cybersikkerhedsforanstaltninger, som er dokumenteret. Prøvninger skal udføres af den godkendende myndighed eller den tekniske tjeneste selv eller i samarbejde med køretøjsfabrikanten ved prøveudtagning. Prøveudtagningen skal være fokuseret på, men ikke begrænset til, risici, der vurderes som værende høje i forbindelse med risikovurderingen.

5.1.3. Den godkendende myndighed eller den tekniske tjeneste skal nægte at meddele typegodkendelse for så vidt angår cybersikkerhed, hvis køretøjsfabrikanten ikke har opfyldt ét eller flere af kravene under punkt 7.3, navnlig hvis:

a) køretøjsfabrikanten ikke har foretaget den i punkt 7.3.3 nævnte udtømmende risikovurdering, herunder i tilfælde, hvor fabrikanten ikke har taget hensyn til alle de risici forbundet med truslerne nævnt i del A i bilag 5.

b) køretøjsfabrikanten ikke har beskyttet køretøjstypen mod de risici, der er identificeret i fabrikantens risikovurdering, eller der ikke er gennemført forholdsmæssige modforanstaltninger som krævet i punkt 7

c) køretøjsfabrikanten ikke har indført passende og forholdsmæssige foranstaltninger til at sikre dedikerede miljøer i køretøjstypen (hvis sådanne findes) til lagring og brug af software, tjenester, applikationer eller data på eftermarkedet

d) køretøjsfabrikanten ikke forud for godkendelsen har foretaget passende og tilstrækkelig prøvning for at kontrollere, at de anvendte sikkerhedsforanstaltninger er effektive.

5.1.4. Den godkendende myndighed, der foretager vurderingen, skal også nægte at meddele typegodkendelse med hensyn til cybersikkerhed, hvis den godkendende myndighed eller den tekniske tjeneste ikke har modtaget tilstrækkelige oplysninger fra køretøjsfabrikanten til at vurdere køretøjstypen med hensyn til cybersikkerhed.

5.2. Meddelelse om godkendelse, udvidelse eller nægtelse af godkendelse af en køretøjstype i henhold til dette regulativ skal gives de kontraherende parter i 1958-overenskomsten, der anvender dette regulativ, ved hjælp af en meddelelse, der er i overensstemmelse med modellen i bilag 2 til dette regulativ.

5.3. De godkendende myndigheder må ikke meddele typegodkendelse uden at kontrollere, at fabrikanten har indført tilfredsstillende ordninger og procedurer til korrekt forvaltning af de cybersikkerhedsaspekter, der er omfattet af dette regulativ.

5.3.1. Den godkendende myndighed og dens tekniske tjenester skal ud over de kriterier, der er fastsat i skema 2 til 1958-overenskomsten, sikre, at de:

a) råder over kompetent personale med passende viden inden for cybersikkerhed og særlig viden om risikovurderinger af køretøjer ([1])

b) har gennemført procedurer for den ensartede evaluering i henhold til dette regulativ.

5.3.2. Alle de kontraherende parter, der anvender dette regulativ, skal gennem deres godkendende myndighed underrette og informere andre godkendende myndigheder hos andre kontraherende parter, der anvender dette FN-regulativ, om de metoder og kriterier, der lægges til grund af den underrettende myndighed med henblik på at vurdere hensigtsmæssigheden af de foranstaltninger, der er truffet i overensstemmelse med dette regulativ, særlig punkt 5.1, 7.2 og 7.3.

Oplysningerne skal udveksles a) lige inden, der meddeles typegodkendelse for første gang i henhold til dette regulativ, og b) hver gang metoden eller kriterierne for vurdering ajourføres.

Oplysningerne er beregnet til at blive udvekslet med henblik på indhentning og analyse af bedste praksis og med henblik på at sikre en ensartet anvendelse af dette regulativ af alle de godkendende myndigheder, der anvender dette regulativ.

5.3.3. Oplysningerne i punkt 5.3.2 skal uploades på engelsk til den sikre internetdatabase "DETA" ([2]), som er oprettet af De Forenede Nationers Økonomiske Kommission for Europa, i god tid og senest 14 dage før en godkendelse meddeles for første gang i henhold til de relevante vurderingsmetoder og -kriterier. Der skal være tilstrækkeligt med oplysninger til at forstå, hvilke mindstekrav til ydeevne, den godkendende myndighed har vedtaget for hvert af de specifikke krav i punkt 5.3.2 samt de processer og foranstaltninger, myndigheden anvender til at efterprøve, at disse mindstekrav til ydeevne er overholdt ([3]).

5.3.4. De godkendende myndigheder, som modtager oplysningerne nævnt i punkt 5.3.2 kan indgive bemærkninger til den underrettende godkendende myndighed ved at uploade dem til DETA senest 14 dage efter dagen for meddelelse af godkendelse.

5.3.5. Såfremt det ikke er muligt for den godkendende myndighed, der meddeler godkendelse, at tage hensyn til de bemærkninger, der er modtaget i henhold til punkt 5.3.4, skal den godkendende myndighed, der har indgivet bemærkningerne, og den godkendende myndighed, der meddeler godkendelse, indhente yderligere oplysninger i overensstemmelse med skema 6 til 1958-aftalen. Den relevante arbejdsgruppe ([4]) under Verdensforummet for Harmonisering af Køretøjsforskrifter (WP.29) for dette regulativ fastsætter en fælles fortolkning af vurderingsmetoder og -kriterier ([5]). Den fælles fortolkning gennemføres, og alle godkendende myndigheder udsteder typegodkendelser i henhold til dette regulativ i overensstemmelse med denne fortolkning.

([1]) F.eks. ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.
([2]) https://www.unece.org/trans/main/wp29/datasharing.html.
([3]) Vejledning for de detaljerede oplysninger (f.eks. metode, kriterier, ydeevne) skal uploades, og formatet skal angives i det fortolkningsdokument, der er under udarbejdelse af taskforcen om indberetning af cybersikkerhed og trådløs transmission i forbindelse med det syvende møde i arbejdsgruppen for automatiserede/selvkørende og opkoblede køretøjer (GRVA).
([4]) Arbejdsgruppen for automatiserede/selvkørende og opkoblede køretøjer (GRVA).
([5]) Fortolkningen skal afspejles i det fortolkningsdokument, der henvises til i fodnoten til punkt 5.3.3.

5.3.6. En godkendende myndighed, der meddeler en typegodkendelse i henhold til dette regulativ, skal underrette de andre godkendende myndigheder om den godkendelse, der er meddelt. Typegodkendelsen og den supplerende dokumentation uploades af den typegodkendende myndighed på engelsk til DETA senest 14 dage efter datoen for godkendelsen ([6]).

5.3.7. De kontraherende parter kan undersøge de godkendelser, der er meddelt på grundlag af de oplysninger, der er uploadet i henhold til punkt 5.3.6. I tilfælde af divergerende holdninger blandt de kontraherende parter, løses dette i overensstemmelse med artikel 10 og skema 6 til 1958-overenskomsten. De kontraherende parter underretter også den relevante arbejdsgruppe i Verdensforummet for Harmonisering af Køretøjsforskrifter (WP.29) om de divergerende fortolkninger i henhold til skema 6 til 1958-overenskomsten. Den relevante arbejdsgruppe bidrager til at finde en løsning hvad angår de forskellige holdninger og kan om nødvendigt rådføre sig med WP.29.

5.4. For så vidt angår punkt 7.2 i dette regulativ skal fabrikanten sikre, at de cybersikkerhedsaspekter, der er omfattet af dette regulativ, gennemføres.

6. Overensstemmelsescertifikat for systemet til forvaltning af cybersikkerhed

6.1. De kontraherende parter udpeger en godkendende myndighed, der skal foretage vurderingen af fabrikanten og udstede et overensstemmelsescertifikat for systemet til forvaltning af cybersikkerhed.

6.2. En ansøgning om et overensstemmelsescertifikat for systemet til forvaltning af cybersikkerhed indgives af køretøjsfabrikanten eller dennes behørigt befuldmægtigede repræsentant.

6.3. Ansøgningen skal bilægges nedennævnte dokumenter i tre eksemplarer og følgende oplysninger:

6.3.1. Dokumenter, der beskriver systemet til forvaltning af cybersikkerhed

6.3.2. En underskrevet erklæring efter den model, der er defineret i tillæg 1 til bilag 1.

6.4. I forbindelse med vurderingen skal fabrikanten ved hjælp af den model, som er defineret i tillæg 1 til bilag 1, erklære og over for den godkendende myndighed og dens tekniske tjeneste på tilfredsstillende vis påvise, at fabrikanten råder over de nødvendige processer for at opfylde alle kravene til cybersikkerhed i henhold til dette regulativ.

6.5. Når denne vurdering er tilfredsstillende gennemført og når der foreligger en underskrevet erklæring fra fabrikanten i overensstemmelse med modellen i tillæg 1 til bilag 1, udstedes der til fabrikanten et certifikat kaldet overensstemmelsescertifikat for systemet til forvaltning af cybersikkerhed som beskrevet i bilag 4 til dette regulativ (i det følgende benævnt CSMS-overensstemmelsescertifikatet).

6.6. Den godkendende myndighed eller dens tekniske tjeneste anvender den model for CSMS-overensstemmelsescertifikatet, der er fastsat i bilag 4 til dette regulativ.

6.7. CSMS-overensstemmelsescertifikatet forbliver gyldig i højst tre år fra datoen for certifikatets udstedelse, med mindre det bliver tilbagekaldt.

6.8. Den godkendende myndighed, der har udstedt CSMS-overensstemmelsescertifikatet, kan til enhver tid kontrollere, at kravene til det fortsat er opfyldt. Den godkendende myndighed tilbagekalder CSMS-overensstemmelsescertifikatet, hvis kravene i dette regulativ ikke længere er opfyldt.

([6]) Yderligere oplysninger om mindstekravene til dokumentationspakken udvikles på det syvende møde i GRVA.

6.9. Fabrikanten skal underrette den godkendende myndighed eller dens tekniske tjeneste om eventuelle ændringer, der påvirker relevansen af CSMS-overensstemmelsescertifikatet. I samråd med fabrikanten afgør den godkendende myndighed eller dens tekniske tjeneste, om nye kontroller er nødvendige.

6.10. For at gøre det muligt for den godkendende myndighed at afslutte sin vurdering inden udløbet af gyldighedsperioden for CSMS-overensstemmelsescertifikatet, skal denne i god tid ansøge om et nyt certifikat eller en forlængelse af det eksisterende CSMS-overensstemmelsescertifikat. Med forbehold for en positiv vurdering udsteder den godkendende myndighed et nyt CSMS-overensstemmelsescertifikat eller forlænger dets gyldighed med yderligere tre år. Den godkendende myndighed kontrollerer, at systemet til forvaltning af cybersikkerhed fortsat opfylder kravene i dette regulativ. Den godkendende myndighed udsteder et nyt certifikat i tilfælde, hvor den godkendende myndighed eller dens tekniske er blevet underrettet om ændringer, og den nye vurdering af disse ændringer er positiv.

6.11. Udløb eller tilbagekaldelse af fabrikantens CSMS-overensstemmelsescertifikat betragtes som en ændring af godkendelsen, jf. punkt 8, for så vidt angår de køretøjstyper, som forvaltningssystemet var relevant for, hvilket kan medføre en tilbagekaldelse af godkendelsen, hvis betingelserne for at opnå godkendelse ikke længere er opfyldt.

7. Specifikationer

7.1. Generelle specifikationer

7.1.1. Kravene i dette regulativ begrænser ikke bestemmelser eller krav i andre FN-regulativer.

7.2. Krav til systemet til forvaltning af cybersikkerhed

7.2.1. Under vurderingen skal den godkendende myndighed eller dens tekniske tjeneste kontrollere, at køretøjsfabrikanten har etableret et system til forvaltning af cybersikkerhed samt, at systemet er i overensstemmelse med dette regulativ.

7.2.2. Systemet til forvaltning af cybersikkerhed skal omfatte følgende aspekter:

7.2.2.1. Køretøjsfabrikanterne skal over for den godkendende myndighed eller den tekniske tjeneste godtgøre, at deres system til forvaltning af cybersikkerhed finder anvendelse på følgende faser:

a) udviklingsfasen

b) produktionsfasen

c) efterproduktionsfasen.

7.2.2.2. Køretøjsfabrikanten skal godtgøre, at de processer, der anvendes af systemet til forvaltning af cybersikkerhed, sikrer, at der tages tilstrækkeligt hensyn til sikkerheden, herunder de risici og modforanstaltninger, der er anført i bilag 5. Dette skal omfatte:

a) de processer, der anvendes i fabrikantens organisation til forvaltning af cybersikkerhed

b) de processer, der anvendes til at identificere risici for køretøjstyper. Under disse processer skal truslerne i del A, bilag 5, og andre relevante trusler tages i betragtning

c) de processer, der anvendes til vurdering, kategorisering og håndtering af de identificerede risici

d) de processer, der er indført for at kontrollere, at de identificerede risici forvaltes hensigtsmæssigt

e) de processer, der anvendes til at afprøve cybersikkerheden af en køretøjstype

f) de processer, der anvendes for at sikre, at risikovurderingen altid er ajourført

g) de processer, der anvendes til at overvåge, opdage og håndtere cyberangreb og cybertrusler mod og sårbarheder i køretøjstyper, og de processer, der anvendes til at vurdere, om de gennemførte cybersikkerheds-foranstaltninger fortsat er effektive i lyset af nye cybertrusler og sårbarheder, der er blevet identificeret

h) de processer, der anvendes til at tilvejebringe relevante data til støtte for analyse af forsøg på cyberangreb eller gennemførte cyberangreb.

7.2.2.3. På grundlag af kategoriseringen i punkt 7.2.2.2, litra c), og 7.2.2.2, litra g), skal køretøjsfabrikanten påvise, at de processer, der anvendes i systemet til forvaltning af cybersikkerhed sikrer, at cybertrusler og -sårbarheder, som kræver en reaktion fra køretøjsfabrikanten, afbødes inden for en rimelig tidsramme.

7.2.2.4. Køretøjsfabrikanten skal påvise, at de processer, der anvendes i systemet til forvaltning af cybersikkerhed sikrer, at overvågningen nævnt i punkt 7.2.2.2, litra g), er kontinuerlig. Dette skal omfatte:

a) overvågning af køretøjer efter første registrering

b) kapacitet til at analysere og opdage cybertrusler, sårbarheder og cyberangreb ud fra køretøjsdata og -logfiler. Denne kapacitet skal overholde bestemmelserne i punkt 1.3 og bilejeres og -brugeres ret til privatlivets fred, især hvad angår samtykke.

7.2.2.5. Hvad angår kravene i punkt 7.2.2.2 skal køretøjsfabrikanten kunne vise, hvordan systemet til forvaltning af cybersikkerhed vil håndtere eventuelle indbyrdes afhængigheder mellem leverandører, tjenesteydere eller fabrikantens underorganisationer.

7.3. Krav til køretøjstyper

7.3.1. Fabrikanten skal være i besiddelse af et gyldigt overensstemmelsescertifikat for systemet til forvaltning af cybersikkerhed, som er relevant for den køretøjstype, der skal godkendes. Hvis køretøjsfabrikanten imidlertid kan påvise, at køretøjstypen ikke kunne udvikles i overensstemmelse med systemet til forvaltning af cybersikkerhed, skal køretøjsfabrikanten, for typegodkendelser af køretøjer i klasse M, N og O først udstedt før den 1. juli 2024, og for typegodkendelser af køretøjer i klasse L først udstedt før den 1. juli 2029, samt for hver udvidelse heraf, godtgøre, at der blev taget tilstrækkeligt hensyn til cybersikkerheden under udviklingsfasen af den pågældende køretøjstype.

7.3.2. Køretøjsfabrikanten skal identificere og forvalte risici forbundet med leverandører for den køretøjstype, der skal godkendes.

7.3.3. Køretøjsfabrikanten skal identificere de kritiske elementer for køretøjstypen og foretage en udtømmende risikovurdering af køretøjstypen og håndtere/forvalte de identificerede risici på passende vis. Risikovurderingen skal tage hensyn til de enkelte elementer af køretøjstypen og vekselvirkninger mellem disse. Risikovurderingen skal endvidere tage hensyn til vekselvirkninger med eventuelle eksterne systemer. I vurderingen af risici skal køretøjsfabrikanten tage hensyn til de risici, der er forbundet med alle de trusler, som nævnes i del A, bilag 5, samt alle andre relevante risici.

7.3.4. Køretøjsfabrikanten skal beskytte køretøjstypen mod de risici, der identificeres i fabrikantens risikovurdering. Der skal gennemføres forholdsmæssige modforanstaltninger med henblik på at beskytte køretøjstypen. De gennemførte modforanstaltninger skal omfatte alle de modforanstaltninger i del B og C i bilag 5, som er relevante for de identificerede risici. Hvis en modforanstaltning nævnt i del B eller C i bilag 5 ikke er relevant eller ikke er tilstrækkelig for den identificerede risiko, skal køretøjsfabrikanten imidlertid sikre, at der gennemføres en anden passende modforanstaltning.

Særligt skal køretøjsfabrikanten, for typegodkendelser af køretøjer i klasse M, N og O først udstedt før den 1. juli 2024, og for typegodkendelser af køretøjer i klasse L først udstedt før den 1. juli 2029, samt for hver udvidelse heraf, sikre, at en anden passende modforanstaltning gennemføres, såfremt det ikke er teknisk muligt at gennemføre en modforanstaltning som omhandlet i del B eller C i bilag 5. Fabrikanten skal stille den respektive vurdering af den tekniske gennemførlighed til rådighed for den godkendende myndighed.

7.3.5. Køretøjsfabrikanten skal indføre passende og forholdsmæssige foranstaltninger til at sikre særlige miljøer i køretøjstypen (hvis sådanne findes) til lagring og brug af software, tjenester, applikationer eller data på eftermarkedet

7.3.6. Køretøjsfabrikanten skal forud for godkendelsen foretage passende og tilstrækkelig prøvning for at kontrollere, at de anvendte sikkerhedsforanstaltninger er effektive.

7.3.7. Køretøjsfabrikanten skal gennemføre foranstaltninger for køretøjstypen med henblik på at:

a) opdage og forebygge cyberangreb mod køretøjer af den pågældende køretøjstype

b) støtte køretøjsfabrikantens overvågningskapacitet hvad angår opdagelse af trusler, sårbarheder og cyberangreb, der er relevante for køretøjstypen

c) tilvejebringe IT-kriminalteknisk kapacitet, der muliggør analyser af forsøg på cyberangreb eller gennemførte cyberangreb.

7.3.8. Kryptografiske moduler, der anvendes i forbindelse med dette regulativ, skal være i overensstemmelse med standarder fastlagt i konsensus. Hvis de anvendte kryptografiske moduler ikke er i overensstemmelse med standarderne fastlagt i konsensus, skal køretøjsfabrikanten begrunde anvendelsen.

7.4. Bestemmelser om rapportering

7.4.1. Køretøjsfabrikanten aflægger mindst én gang om året eller oftere, om nødvendigt, rapport til den godkendende myndighed eller den tekniske tjeneste om resultatet af deres overvågningsaktiviteter som defineret i punkt 7.2.2.2, litra g); rapporteringen skal omfatte relevante oplysninger om nye cyberangreb. Køretøjsfabrikanten skal også rapportere og bekræfte over for den godkendende myndighed eller den tekniske tjeneste, at de gennemførte modforanstaltninger mod cyberangreb for sine køretøjstyper fortsat er effektive, samt om der er truffet eventuelle yderligere foranstaltninger.

7.4.2. Den godkendende myndighed eller den tekniske tjeneste skal kontrollere de leverede oplysninger og om nødvendigt kræve, at køretøjsfabrikanten afhjælper al påvist ineffektivitet.

Hvis rapporteringen eller afhjælpningen ikke er tilstrækkelig, kan den godkendende myndighed beslutte at tilbagekalde CSMS-overensstemmelsescertifikatet, jf. punkt 6.8.

8. Ændring af køretøjstypen og udvidelse af typegodkendelsen

8.1. Enhver ændring af køretøjstypen, som påvirker dens tekniske ydeevne med hensyn til cybersikkerheden og/eller den dokumentation, der er påkrævet i henhold til dette regulativ, skal meddeles den godkendende myndighed, der har godkendt køretøjstypen. Den godkendende myndighed kan da enten:

8.1.1. vurdere, at de foretagne ændringer stadig overholder kravene til og dokumentation af den eksisterende typegodkendelse eller

8.1.2. foretage den nødvendige supplerende vurdering i henhold til punkt 5 og, hvis det er relevant, kræve en yderligere prøvningsrapport fra den tekniske tjeneste, der er ansvarlig for udførelsen af prøvninger.

8.1.3. Bekræftelse, udvidelse eller nægtelse af godkendelse, med angivelse af ændringerne, meddeles ved hjælp af en meddelelsesformular, der er i overensstemmelse med modellen i bilag 2 til dette regulativ. Den godkendende myndighed, som udsteder udvidelse af en godkendelse, tildeler udvidelsen et serienummer og underretter de andre parter i 1958-overenskomsten, der anvender dette regulativ, ved hjælp af en meddelelsesformular, der er i overensstemmelse med modellen i bilag 2 til dette regulativ.

9. Produktionens overensstemmelse

9.1. Procedurerne til sikring af produktionens overensstemmelse skal opfylde forskrifterne i 1958-overenskomstens skema 1 (E/ECE/TRANS/505/Rev.3), idet følgende forskrifter finder anvendelse:

9.1.1. Indehaveren af godkendelsen skal sikre, at resultaterne af prøvningerne af produktionens overensstemmelse registreres, og at de vedlagte dokumenter er tilgængelige i en periode, der fastsættes efter aftale med den godkendende myndighed eller dens tekniske tjeneste. Denne periode må ikke overstige 10 år regnet fra tidspunktet for produktionens endelige ophør.

9.1.2. Den godkendende myndighed, som har meddelt typegodkendelsen, kan til enhver tid kontrollere de metoder til overensstemmelseskontrol, der anvendes på de enkelte produktionsanlæg. Der foretages normalt en inspektion hvert tredje år.

10. Sanktioner i tilfælde af produktionens manglende overensstemmelse

10.1. Den godkendelse, der meddeles for en køretøjstype i henhold til dette regulativ, kan inddrages, hvis forskrifterne i dette regulativ ikke overholdes, eller hvis prøvekøretøjerne ikke overholder forskrifterne i dette regulativ.

10.2. Hvis den godkendende myndighed inddrager en godkendelse, som den tidligere har meddelt, skal den straks underrette de øvrige kontraherende parter, der anvender dette regulativ, herom ved hjælp af en meddelelsesformular, der er i overensstemmelse med modellen i bilag 2 til dette regulativ.

11. Endeligt ophør af produktionen

11.1. Hvis indehaveren af godkendelsen endeligt ophører med at fremstille en køretøjstype, som er godkendt i henhold til dette regulativ, underretter indehaveren den myndighed, som har meddelt godkendelsen, herom. Ved modtagelse af den relevante meddelelse skal den pågældende myndighed meddele dette til de andre kontraherende parter i overenskomsten, der anvender dette regulativ, ved hjælp af en kopi af godkendelsesformularen, som i slutningen med store typer er forsynet med den underskrevne og daterede påskrift "PRODUKTION OPHØRT".

12. Navne og adresser på tekniske tjenester, som er ansvarlige for udførelse af godkendelsesprøvning, og på de typegodkendende myndigheder

12.1. De kontraherende parter i overenskomsten, som anvender dette regulativ, meddeler De Forenede Nationers sekretariat navnene og adresserne på de tekniske tjenester, som udfører typegodkendelsesprøvninger, og på de typegodkendende myndigheder, som meddeler typegodkendelser, og hvortil meddelelser om typegodkendelse eller udvidelse, nægtelse eller inddragelse af typegodkendelse, der er udstedt i andre lande, skal sendes.

BILAG 1

Oplysningsskema

Følgende oplysninger skal i de relevante tilfælde indsendes i tre eksemplarer og omfatte en indholdsfortegnelse. Eventuelle tegninger skal forelægges i en passende målestok på A4-ark eller foldet til dette format. Eventuelle fotografier skal være tilstrækkeligt detaljerede.

1. Fabrikat (fabrikantens handelsbetegnelse):.....

2. Type og almindelig(e) handelsbetegnelse(r):.....

3. Typeidentifikationsmærke, hvis markeret på køretøjet:.....

4. Mærkets anbringelsessted: .....

5. Køretøjskategori(er):.....

6. Navn og adresse på fabrikanten/fabrikantens repræsentant:.....

7. Navne og adresser på samlefabrikker: .....

8. Fotografier og/eller tegninger af et repræsentativt køretøj: .....

9. Cybersikkerhed

9.1. Almindelige specifikationer for køretøjstypen, herunder:

a) køretøjssystemer, som er relevante for køretøjstypens cybersikkerhed

b) komponenterne i de systemer, der er relevante for cybersikkerheden

c) vekselvirkninger mellem disse systemer og andre systemer inden for køretøjstypen og eksterne grænseflader.

9.2. Skematisk fremstilling af køretøjstypen

9.3. Nummer på CSMS-overensstemmelsescertifikatet: .....

9.4. Dokumenter for den køretøjstype, der skal godkendes, som indeholder en beskrivelse af resultatet af risikovurderingen og de identificerede risici:.....

9.5. Dokumenter for den køretøjstype, der skal godkendes, som indeholder en beskrivelse af de modforanstaltninger, der er gennemført for de anførte systemer eller for køretøjstypen, og hvordan de håndterer de angivne risici: .....

9.6. Dokumenter for den køretøjstype, der skal godkendes, som indeholder en beskrivelse af beskyttelse af særlige miljøer til lagring og brug af software, tjenester, applikationer eller data på eftermarkedet:.....

9.7. Dokumenter for den køretøjstype, der skal godkendes, som indeholder en beskrivelse af, hvilke prøvninger der er foretaget for at kontrollere cybersikkerheden af køretøjstypen og dens systemer samt resultatet af disse prøvninger:.....

9.8. Beskrivelse af gennemgangen af forsyningskæden med hensyn til cybersikkerhed:.....

Bilag 1 — Tillæg 1

Model for fabrikantens erklæring om overensstemmelse for systemet til forvaltning af cybersikkerhed

Fabrikantens erklæring om overensstemmelse med kravene til systemet til forvaltning af cybersikkerhed

Fabrikantens navn:……

Fabrikantens adresse: ……

……(*Fabrikantens navn*)

erklærer, at de nødvendige processer til opfyldelse af kravene til systemet til forvaltning af cybersikkerhed fastsat i punkt 7.2 i FN-regulativ 155 er blevet installeret og vil blive vedligeholdt.

Udfærdiget i: …… (*sted*)

Dato:……

Underskriverens navn:……

Underskriverens funktion:……

(Fabrikantens repræsentant, stempel og underskrift)

BILAG 2

Meddelelse

(Største format: A4 (210 × 297 mm))



Udstedt af: Myndighedens navn:
.....
.....
.....

Vedrørende (2): Meddelelse af godkendelse
Udvidelse af godkendelse
Inddragelse af godkendelse med virkning fra dd.mm.åååå
Nægtelse af godkendelse
Endeligt ophør af produktionen

for en køretøjstype i henhold til FN-regulativ nr. 155

Godkendelse nr.:.....

Udvidelse nr.: .....

Begrundelse for udvidelsen:.....

1. Fabrikat (fabrikantens handelsbetegnelse):.....

2. Type og almindelig(e) handelsbetegnelse(r):.....

3. Typeidentifikationsmærke, hvis markeret på køretøjet:.....

3.1. Mærkets anbringelsessted: .....

4. Køretøjskategori(er):.....

5. Navn og adresse på fabrikanten/fabrikantens repræsentant:.....

6. Navn(e) og adresse(r) på produktionsanlæg.....

7. Nummer på overensstemmelsescertifikatet for systemet til forvaltning af cybersikkerhed:.....

8. Teknisk tjeneste, som er ansvarlig for udførelse af prøvningen:.....

9. Prøvningsrapportens dato: .....

10. Prøvningsrapportens nummer:.....

11. Bemærkninger: (hvis relevant) .....

12. Sted: .....

(1) Kendingsnummer for det land, hvor godkendelsen er meddelt/udvidet/nægtet/inddraget (se godkendelsesforskrifter i regulativet).
(2) Det ikke gældende overstreges.

13. Dato:……

14. Underskrift:……

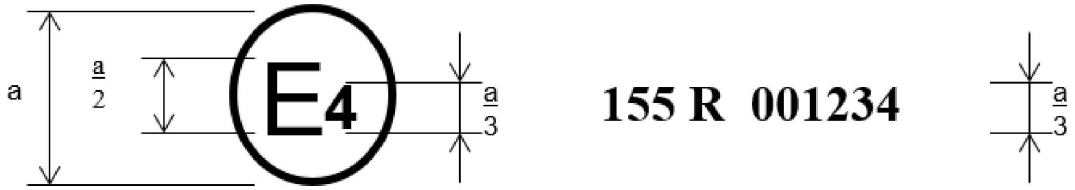
15. Indholdsfortegnelsen til den informationspakke, der er indgivet til den godkendende myndighed, og som kan fås ved henvendelse dertil, er vedlagt:

BILAG 3

Godkendelsesmærkets udformning

MODEL A

(Se punkt 4.2 i dette regulativ)



a = 8 mm min.

Ovenstående godkendelsesmærke, som er påført et køretøj, viser, at den pågældende køretøjstype er godkendt i Nederlandene (E 4) i henhold til regulativ nr. 155 under godkendelsesnummer 001234. De første to cifre i godkendelsesnummeret angiver, at godkendelsen blev meddelt i overensstemmelse med kravene i regulativet i dets oprindelige (00) udgave.

BILAG 4

MODEL FOR CSMS-OVERENSSTEMMELSESCERTIFIKATET

Overensstemmelsescertifikat for systemet til forvaltning af cybersikkerhed

i henhold til FN-regulativ nr. 155

Certifikatnummer [*referencenummer*]

[… *Godkendende myndighed*]

bekræfter hermed, at

Fabrikant: ……

Fabrikantens adresse: ……

overholder bestemmelserne i punkt 7.2 i regulativ nr. 155

Kontrol er udført den: ……

af (navn og adresse på den godkendende myndighed eller tekniske tjeneste): ……

Rapportens nummer: ……

Certifikatet er gyldigt til den […… *dato*]

Udstedt i […… *sted*]

Den […… *dato*]

[…… *underskrift*]

Bilag: Fabrikantens beskrivelse af systemet til forvaltning af cybersikkerhed.

BILAG 5

Liste over trusler og tilknyttede modforanstaltninger

1. Dette bilag består af tre dele. Del A i dette bilag beskriver referencescenarier for trusler, sårbarheder og angrebsmetoder. Del B i dette bilag beskriver modforanstaltninger mod trusler, der er rettet mod køretøjstyper. Del C beskriver modforanstaltninger med trusler, der er rettet mod områder uden for køretøjer, dvs. mod backend-IT.

2. Del A, del B og del C skal tages i betragtning i forbindelse med risikovurderingen og de modforanstaltninger, der skal gennemføres af køretøjsfabrikanterne.

3. Beskrivelsen af sårbarheden på højt niveau og de tilsvarende eksempler er indekseret i del A. Den samme indeksering er angivet i tabellerne i del B og C for at kæde hvert enkelt angreb eller hver enkelt sårbarhed sammen med en liste over tilsvarende modforanstaltninger.

4. Trusselsanalysen skal også tage højde for mulige konsekvenser af angrebet. Disse konsekvenser kan være med til at fastslå, hvor alvorlig en risiko er, samt identificere yderligere risici. Mulige angreb kan have følgende konsekvenser:

   a) sikker drift af køretøjet påvirkes

   b) køretøjsfunktioner ophører med at fungere

   c) software modificeres, ydeevnen ændres

   d) software ændres, men der er ingen driftspåvirkninger

   e) brud på dataintegritet

   f) brud på datafortrolighed

   g) tab af datatilgængelighed

   h) andet, herunder kriminalitet.

DEL A

Sårbarhed eller angrebsmetode i tilknytning til trusler

Beskrivelser på højt niveau af trusler og tilknyttede sårbarheder eller angrebsmetoder er anført i tabel A1.

Tabel A1

Liste over sårbarheder eller angrebsmetoder i forbindelse med trusler

Beskrivelse af sårbarhed/trussel på højt niveau og underniveau			Eksempel på sårbarhed eller angrebsmetode	
4.3.1. Trusler fra backend-servere mod køretøjer i drift	1	Backend-servere anvendes som et middel til at angribe et køretøj eller udtrække data fra det	1.1	Misbrug af privilegier blandt ansatte (insiderangreb)
			1.2	Uautoriseret internetadgang til serveren (f.eks. via bagdøre, sikkerhedshuller i systemsoftware, SQL-angreb eller andre midler)
			1.3	Uautoriseret fysisk adgang til serveren (f.eks. vha. USB-nøgler eller andre medier, der er forbundet med serveren)
	2	Tjenester fra backend-serveren bliver afbrudt og påvirker driften af et køretøj	2.1	Angreb på backend-serveren stopper driften af serveren, f.eks. kan angrebet forhindre serveren i at interagere med køretøjer og levere de nødvendige tjenester

Beskrivelse af sårbarhed/trussel på højt niveau og underniveau			Eksempel på sårbarhed eller angrebsmetode	
	3	Data vedrørende køretøjet på backend-servere går tabt eller kompromitteres ("databrud")	3.1	Misbrug af privilegier blandt ansatte (insiderangreb)
			3.2	Tab af oplysninger i skyen. Følsomme data kan gå tabt på grund af angreb eller ulykker, når data lagres af tredjepartsudbydere af cloudtjenester
			3.3	Uautoriseret internetadgang til serveren (f.eks. via bagdøre, sikkerhedshuller i systemsoftware, SQL-angreb eller andre midler)
			3.4	Uautoriseret fysisk adgang til serveren (f.eks. vha. USB-nøgler eller andre medier, der er forbundet med serveren)
			3.5	Informationsbrud via utilsigtet udveksling af data (f.eks. administratorfejl)
4.3.2 Trusler mod køretøjer via deres kommunikationskanaler	4	Spoofing af meddelelser eller data modtaget af køretøjet	4.1	Spoofing af meddelelser ved anvendelse af falsk identitet (f.eks. CA- og manøvrekoordinering via V2X-meddelelser, GNSS-meddelelser mm.)
			4.2	Sybil-angreb (med henblik på at spoofe andre køretøjer og få det til at se ud som om, der er mange køretøjer på vejen)
	5	Kommunikationskanaler anvendes til uautoriseret manipulation, sletning eller andre ændringer af kode/data i køretøjet	5.1	Kommunikationskanaler gør det muligt at indsætte koder, f.eks. kan manipulerede binære softwarefiler indsættes i kommunikationsstrømmen
			5.2	Kommunikationskanaler gør det muligt at manipulere med data/kode i køretøjet
			5.3	Kommunikationskanaler gør det muligt at overskrive data/kode i køretøjet
			5.4	Kommunikationskanaler gør det muligt at slette data/kode i køretøjet
			5.5	Kommunikationskanaler gør det muligt at introducere data/kode i køretøjet (skrive datakode)
	6	Kommunikationskanaler accepterer usikre/upålidelige beskeder eller er sårbare over for session hijacking/replay-angreb	6.1	Accept af oplysninger fra en upålidelig eller usikker kilde
			6.2	"Man-in-the-middle"-angreb/session hijacking
			6.3	Replay-angreb, f.eks. et angreb mod en kommunikationsgateway, gør det muligt for angriberen at nedklassificere software fra gatewayens ECU eller firmware
	7	Oplysninger kan nemt videregives, f.eks. gennem aflytning af kommunikation eller uautoriseret adgang til følsomme filer eller mapper	7.1	Opsnapning af oplysninger/forstyrrende stråling/overvågning af kommunikation
			7.2	Opnåelse af uautoriseret adgang til filer eller data

Beskrivelse af sårbarhed/trussel på højt niveau og underniveau			Eksempel på sårbarhed eller angrebsmetode	
	8	Denial of service-angreb via kommunikationskanaler med henblik på at forstyrre køretøjets drift	8.1	Afsendelse af en stor mængde unyttige data til køretøjets informationssystem, så det ikke er i stand til at levere tjenester på normal vis
			8.2	Black hole-angreb, angriberen er i stand til at blokere for meddelelser mellem køretøjerne for at forstyrre kommunikationen mellem køretøjer
	9	En ikkeprivilegeret bruger kan få privilegeret adgang til køretøjssystemerne	9.1	En ikkeprivilegeret bruger kan få privilegeret adgang, f.eks. root-adgang
	10	Virus skjult i kommunikationsmedier kan inficere køretøjssystemerne	10.1	Virus skjult i kommunikationsmedier inficerer køretøjssystemerne
	11	Meddelelser, der modtages af køretøjet (f.eks. X2V eller diagnosemeddelelser), eller som overføres i selve køretøjet, indeholder skadeligt indhold	11.1	Skadelige interne meddelelser (f.eks. CAN)
			11.2	Skadelige V2X-meddelelser , f.eks. meddelelser fra infrastrukturen til køretøjet eller køretøjer imellem (f.eks. CAM, DENM)
			11.3	Skadelige diagnosemeddelelser
			11.4	Skadelige fortrolige meddelelser (f.eks. meddelelser, der normalt sendes fra OEM eller komponent-/system-/funktions-leverandører)
4.3.3. Trusler mod køretøjer i forbindelse med opdaterings-procedurer	12	Misbrug eller kompromittering af opdateringsprocedurer	12.1	Kompromittering af trådløse softwareopdateringsprocesser. Dette omfatter forfalskning af programmet til systemopdatering eller firmware
			12.2	Kompromittering af lokale/fysiske softwareopdateringsprocesser. Dette omfatter forfalskning af programmet til systemopdatering eller firmware
			12.3	Softwaren manipuleres før opdateringsprocessen (og er derfor beskadiget), men opdateringsprocessen er intakt.
			12.4	Kompromittering af softwareudbyderens kryptografiske nøgler med henblik på at gøre det muligt at foretage en ugyldig opdatering
	13	Det er muligt at nægte gyldige opdateringer	13.1	Denial of Service-angreb mod opdateringsserveren eller netværket for at forhindre udrulningen af kritiske softwareopdateringer og/eller frigivelsen af kundespecifikke funktioner
4.3.4. Trusler mod køretøjer via utilsigtede menneskelige aktiviteter, der fremmer et cyberangreb	15	Legitime aktører kan foretage handlinger, der uforvarende kan lette et cyberangreb	15.1	Uskyldigt offer (f.eks. ejer, bruger eller vedligeholdelsesingeniør), der bliver narret til at foretage en handling og utilsigtet uploade malware eller muliggøre et angreb
			15.2	De definerede sikkerhedsprocedurer bliver ikke fulgt

Beskrivelse af sårbarhed/trussel på højt niveau og underniveau			Eksempel på sårbarhed eller angrebsmetode	
4.3.5. Trusler mod køretøjer via ekstern konnektivitet og eksterne forbindelser	16	Manipulation af køretøjsfunktionernes konnektivitet gør det muligt at gennemføre et cyberangreb. Dette kan omfatte telematik, systemer, der muliggør fjerndrift og systemer, der anvender trådløs kommunikation med kort rækkevidde	16.1	Manipulation af funktioner, der er designet til at fjernbetjene systemer, som f.eks. bilnøgler med fjernbetjening, startspærre og ladestationer
			16.2	Manipulation af køretøjstelematik (f.eks. manipulation af temperaturmåling af følsomme varer, fjernåbning af døre til lastrum)
			16.3	Interferens med trådløse systemer med kort rækkevidde eller sensorer
	17	Hostet software fra tredjepartsleverandører, f.eks. underholdningsapplikationer, anvendes som et middel til at angribe køretøjssystemer	17.1	Beskadigede applikationer, eller applikationer med lav softwaresikkerhed, anvendes som et middel til at angribe køretøjssystemer
	18	Udstyr forbundet med eksterne grænseflader, f.eks. USB-porte, OBD-port, anvendt som et middel til at angribe køretøjssystemer	18.1	Eksterne grænseflader såsom USB-porte eller andre porte anvendes som et angrebspunkt, f.eks. gennem indsættelse af koder
			18.2	Medier, der er inficeret med et virus, forbindes til et køretøjssystem
			18.3	Adgang via diagnosticering (f.eks. dongles i OBD-porte) anvendes til at fremme et angreb, dvs. manipulere køretøjsparametre (direkte eller indirekte)
4.3.6. Trusler mod køretøjsdata/kode	19	Udtrækning af køretøjets data/kode	19.1	Udtrækning af copyright eller ophavsretligt beskyttet software fra køretøjssystemer (plagiering)
			19.2	Uautoriseret adgang til ejerens personoplysninger, f.eks. personidentitet, oplysninger om betalingskonti, adressebog, geografisk placering, køretøjets elektroniske ID osv.
			19.3	Udtrækning af krypteringsnøgler
	20	Manipulation af køretøjets data/kode	20.1	Ulovlig/uautoriseret ændring af køretøjets elektroniske ID
			20.2	Identitetsbedrageri, f.eks. når en bruger ønsker at vise en anden identitet ved kommunikation med vejafgiftssystemer, backend-servere hos fabrikanten
			20.3	Handlinger, der foretages for at omgå overvågningssystemer (f.eks. hacking/manipulation/blokering af meddelelser såsom ODR Tracker data, eller antal kørsler)
			20.4	Datamanipulation med henblik på at forfalske kørselsdata (f.eks. kilometerstand, hastighed, vejvisning mm.)
			20.5	Uautoriserede ændringer af systemdiagnosedata
	21	Sletning af data/kode	21.1	Uautoriseret sletning/manipulation af systemhændelseslog
	22	Introduktion af malware	22.2	Introduktion af skadelig software eller ondsindet softwareaktivitet

Beskrivelse af sårbarhed/trussel på højt niveau og underniveau			Eksempel på sårbarhed eller angrebsmetode	
	23	Introduktion af ny software eller overskrivning af eksisterende software	23.1	Forfalskning af software til køretøjskontrolsystemer eller informationssystemer
	24	Forstyrrelse af systemer eller operationer	24.1	Denial of Service, der f.eks. kan udløses på det interne netværk ved at oversvømme en CAN-bus eller ved at fremprovokere fejl på en ECU via et højt antal beskeder
	25	Manipulation af køretøjsparametre	25.1	Uautoriseret adgang med henblik på forfalskning af konfigurationsparametre for nøglefunktioner i køretøjet, som f.eks. bremsedata, grænseværdi for udløsning af airbag osv.
			25.2	Uautoriseret adgang med henblik på forfalskning af ladeparametre, som f.eks. ladespænding, ladeeffekt, batteritemperatur osv.
4.3.7. Potentielle sårbarheder, der kan udnyttes, hvis de ikke er tilstrækkeligt beskyttede eller hærdede	26	Kryptografiske teknologier kan kompromitteres eller anvendes i utilstrækkelig grad	26.1	En kombination af kortvarige krypteringsnøgler og en lang gyldighedsperiode gør det muligt for angriberen at bryde krypteringen
			26.2	Utilstrækkelig brug af kryptografiske algoritmer til beskyttelse af følsomme systemer
			26.3	Anvendelse af allerede eller snart forældede krypteringsalgoritmer
	27	Dele eller leveringer kan kompromitteres for at gøre det muligt at angribe køretøjet	27.1	Hardware eller software, som er designet til at muliggøre et angreb eller som ikke opfylder konstruktionskriterierne for at standse et angreb
	28	Software eller hardwareudvikling skaber sårbarheder	28.1	Softwarefejl. Tilstedeværelsen af softwarefejl kan være et grundlag for en potentiel udnyttelse af sårbarheder. Dette gælder især, hvis softwaren ikke er blevet testet for at kontrollere, at den ikke er behæftet med kendt dårlig kode/fejl, således at risikoen for tilstedeværelsen af sådanne reduceres
			28.2	Brug af elementer fra udviklingsfasen (f.eks. fejlfindingsporte, JTAG-porte, mikroprocessorer, udviklingscertifikater, udviklingspasswords osv.) kan give adgang til ECU'er eller give angribere mulighed for at få større privilegier
	29	Netværksudformning skaber sårbarheder	29.1	Overflødige åbne internetporte som giver adgang til netværkssystemer
			29.2	Omgåelse af netværksadskillelse med henblik på at opnå kontrol. Et specifikt eksempel herpå er brugen af ubeskyttede gateways eller adgangspunkter (f.eks. gateways mellem lastbil og påhængskøretøj) for at omgå beskyttelse og få adgang til andre netværkssegmenter med henblik på at udføre ondsindede handlinger, som f.eks. afsendelse af vilkårlige CAN-bus-beskeder
	31	Utilsigtet overførsel af data kan forekomme	31.1	Informationsbrud. Personlige data kan lækkes ved ejer- eller brugerskift (dvs. bilen sælges eller bruges som udlejningsbil med nye lejere)

Beskrivelse af sårbarhed/trussel på højt niveau og underniveau			Eksempel på sårbarhed eller angrebsmetode	
	32	Fysisk manipulation af systemer kan muliggøre angreb	32.1	Manipulation af elektronisk hardware, dvs. uautoriseret elektronisk hardware tilføjet til køretøj for at muliggøre "man-in-the-middle"-angreb Udskiftning af autoriseret elektronisk hardware (f.eks. sensorer) med uautoriseret elektronisk hardware Manipulation af oplysninger indsamlet af en sensor (f.eks. anvendelse af en magnet til at forstyrre Hall-effekt-føleren, der er forbundet med gearkassen)

DEL B

Modforanstaltninger til modvirkning af trusler mod køretøjer

1. Modforanstaltninger vedrørende "køretøjets kommunikationskanaler"

Modforanstaltninger mod trusler, som vedrører "køretøjets kommunikationskanaler" er opført i tabel B1.

Tabel B1

Modforanstaltninger mod trusler, som vedrører "køretøjets kommunikationskanaler"

Tabel A1 reference	Trusler mod "køretøjets kommunikationskanaler"	Ref.	Modforanstaltning
4.1	Spoofing af meddelelser (f.eks. CA- og manøvrekoordinering via V2X-meddelelser, GNSS-meddelelser mm.) ved anvendelse af falsk identitet	M10	Køretøjet skal kontrollere autenticiteten og integriteten af de modtagne beskeder
4.2	Sybil-angreb (med henblik på at spoofe andre køretøjer og få det til at se ud som om, der er mange køretøjer på vejen)	M11	Der skal udføres sikkerhedskontrol i forbindelse med lagring af krypteringsnøgler (dvs. anvendelse af hardwaresikkerhedsmoduler)
5.1	Kommunikationskanaler gør det muligt at indsætte koder i køretøjets data/kode, f.eks. kan manipulerede binære softwarefiler indsættes i kommunikationsstrømmen	M10 M6	Køretøjet skal kontrollere autenticiteten og integriteten af de modtagne beskeder Systemer skal implementere indbygget sikkerhed for at minimere risici
5.2	Kommunikationskanaler gør det muligt at manipulere med data/kode i køretøjet	M7	Teknikker til og udformning af adgangskontrol skal anvendes til beskyttelse af systemdata/-kode
5.3	Kommunikationskanaler gør det muligt at overskrive data/kode i køretøjet		
5.4 21.1	Kommunikationskanaler gør det muligt at slette data/kode i køretøjet		
5.5	Kommunikationskanaler gør det muligt at introducere data/kode i køretøjssystemerne (skrive datakode)		

Tabel A1 reference	Trusler mod "køretøjets kommunikationskanaler"	Ref.	Modforanstaltning
6.1	Accept af oplysninger fra en upålidelig eller usikker kilde	M10	Køretøjet skal kontrollere autenticiteten og integriteten af de modtagne beskeder
6.2	"Man-in-the-middle"-angreb/session hijacking	M10	Køretøjet skal kontrollere autenticiteten og integriteten af de modtagne beskeder
6.3	Replay-angreb, f.eks. et angreb mod en kommunikationsgateway, gør det muligt for angriberen at nedklassificere software fra gatewayens ECU eller firmware		
7.1	Opsnapning af oplysninger/forstyrrende stråling/overvågning af kommunikation	M12	Fortrolige data, der sendes til eller fra køretøjet, skal beskyttes
7.2	Opnåelse af uautoriseret adgang til filer eller data	M8	Gennem systemdesign og adgangskontrol bør det være umuligt for uautoriseret personale at få adgang til personlige eller systemkritiske data Eksempler på sikkerhedskontrol kan findes i OWASP
8.1	Afsendelse af en stor mængde unyttige data til køretøjets informationssystem, så det ikke er i stand til at levere tjenester på normal vis	M13	Der skal anvendes foranstaltninger, der gør det muligt at opdage og rette op på et Denial of Service-angreb
8.2	Black hole-angreb, afbrydelse af kommunikationen mellem køretøjer ved at blokere overførslen af beskeder til andre køretøjer	M13	Der skal anvendes foranstaltninger, der gør det muligt at opdage og rette op på et Denial of Service-angreb
9.1	En ikkeprivilegeret bruger kan få privilegeret adgang, f.eks. root-adgang	M9	Der skal anvendes foranstaltninger til forebyggelse og opdagelse af uautoriseret adgang
10.1	Virus skjult i kommunikationsmedier inficerer køretøjssystemerne	M14	Foranstaltninger til beskyttelse af systemer mod indlejrede vira/malware bør overvejes
11.1	Skadelige interne meddelelser (f.eks. CAN)	M15	Foranstaltninger til afsløring af skadelige interne meddelelser bør overvejes
11.2	Skadelige V2X-meddelelser, f.eks. meddelelser fra infrastrukturen til køretøjet eller køretøjer imellem (f.eks. CAM, DENM)	M10	Køretøjet skal kontrollere autenticiteten og integriteten af de modtagne beskeder
11.3	Skadelige diagnosemeddelelser		
11.4	Skadelige fortrolige meddelelser (f.eks. meddelelser, der normalt sendes fra OEM eller komponent-/system-/funktions-leverandører)		

2. Modforanstaltninger vedrørende "opdateringsprocessen"

Modforanstaltninger mod trusler, som vedrører "opdateringsprocessen" er opført i tabel B2.

Tabel B2

Modforanstaltninger mod trusler, som vedrører "opdateringsprocessen"

Tabel A1 reference	Trusler mod "opdateringsprocessen"	Ref.	Modforanstaltning
12.1	Kompromittering af trådløse softwareopdateringsprocesser. Dette omfatter forfalskning af programmet til systemopdatering eller firmware	M16	Der skal anvendes sikre softwareopdateringsprocesser
12.2	Kompromittering af lokale/fysiske softwareopdateringsprocesser. Dette omfatter forfalskning af programmet til systemopdatering eller firmware		
12.3	Softwaren manipuleres før opdateringsprocessen (og er derfor beskadiget), men opdateringsprocessen er intakt.		
12.4	Kompromittering af softwareudbyderens kryptografiske nøgler med henblik på at gøre det muligt at foretage en ugyldig opdatering	M11	Der skal udføres sikkerhedskontrol i forbindelse med lagring af krypteringsnøgler
13.1	Denial of Service-angreb mod opdateringsserveren eller netværket for at forhindre udrulningen af kritiske softwareopdateringer og/eller frigivelsen af kundespecifikke funktioner	M3	Der skal udføres sikkerhedskontrol på backend-systemer. I tilfælde, hvor backend-servere er af afgørende betydning for leveringen af tjenester, eksisterer der backup-procedurer i tilfælde af systemnedbrud. Eksempler på sikkerhedskontrol kan findes i OWASP

3. Modforanstaltninger vedrørende "utilsigtede menneskelige handlinger, der fremmer et cyberangreb"

Modforanstaltninger mod trusler, som vedrører "utilsigtede menneskelige handlinger, der fremmer et cyberangreb" er opført i tabel B3.

Tabel B3

Modforanstaltninger mod trusler, som vedrører "utilsigtede menneskelige handlinger, der fremmer et cyberangreb"

Tabel A1 reference	Trusler vedrørende "utilsigtede menneskelige handlinger"	Ref.	Modforanstaltning
15.1	Et uskyldigt offer (f.eks. ejer, bruger eller vedligeholdelsesingeniør) bliver narret til at foretage en handling og utilsigtet uploade malware eller muliggøre et angreb	M18	Der skal gennemføres foranstaltninger, der definerer og kontrollerer brugerroller og adgangsrettigheder, baseret på princippet om mindst mulig adgang

Tabel A1 reference	Trusler vedrørende "utilsigtede menneskelige handlinger"	Ref.	Modforanstaltning
15.2	De definerede sikkerhedsprocedurer bliver ikke fulgt	M19	Organisationerne skal sørge for, at der er defineret sikkerhedsprocedurer, og at disse bliver fulgt, herunder registrering af handlinger og adgang forbundet med forvaltning af sikkerhedsfunktioner

4. Modforanstaltninger vedrørende "ekstern konnektivitet og eksterne forbindelser"

Modforanstaltninger mod trusler, der vedrører "ekstern konnektivitet og eksterne forbindelser" er opført i tabel B4.

Tabel B4

Modforanstaltninger mod trusler, der vedrører "ekstern konnektivitet og eksterne forbindelser"

Tabel A1 reference	Trusler vedrørende "ekstern konnektivitet og eksterne forbindelser"	Ref.	Modforanstaltning
16.1	Manipulation af funktioner, der er designet til at fjernbetjene køretøjssystemer, som f.eks. bilnøgler med fjernbetjening, startspærre og ladestationer	M20	Der skal udføres sikkerhedskontrol for systemer med fjernadgang
16.2	Manipulation af køretøjstelematik (f.eks. manipulation af temperaturmåling af følsomme varer, fjernåbning af døre til lastrum)		
16.3	Interferens med trådløse systemer med kort rækkevidde eller sensorer		
17.1	Beskadigede applikationer, eller applikationer med lav softwaresikkerhed, anvendes som et middel til at angribe køretøjssystemer	M21	Software skal være sikkerhedsvurderet, bekræftet og integritetsbeskyttet. Der skal udføres sikkerhedskontrol for at minimere risikoen ved software fra tredjemand, som er beregnet til eller forventes at blive hostet i køretøjet
18.1	Eksterne grænseflader såsom USB-porte eller andre porte anvendes som et angrebspunkt, f.eks. gennem indsættelse af koder	M22	Der skal udføres sikkerhedskontrol for eksterne grænseflader
18.2	Medier inficeret med virus, der forbindes med et køretøjssystem		
18.3	Adgang via diagnosticering (f.eks. dongles i OBD-porte) anvendes til at fremme et angreb, dvs. manipulere køretøjsparametre (direkte eller indirekte)	M22	Der skal udføres sikkerhedskontrol for eksterne grænseflader

5. Modforanstaltninger vedrørende "potentielle mål for eller motiver til et angreb"

Modforanstaltninger mod trusler, der vedrører "potentielle mål for eller motiver til et angreb" er opført i tabel B5.

Tabel B5

Modforanstaltninger mod trusler, der vedrører "potentielle mål for eller motiver til et angreb"

Tabel A1 reference	Trusler vedrørende "potentielle mål for eller motiver til et angreb"	Ref.	Modforanstaltning
19.1	Udtrækning af copyright eller ophavsretligt beskyttet software fra køretøjssystemer (plagiering/stjålet software)	M7	Teknikker til og udformning af adgangskontrol skal anvendes til beskyttelse af systemdata/-kode. Eksempler på sikkerhedskontrol kan findes i OWASP
19.2	Uautoriseret adgang til ejerens personoplysninger, f.eks. personidentitet, oplysninger om betalingskonti, adressebog, geografisk placering, køretøjets elektroniske ID osv.	M8	Gennem systemdesign og adgangskontrol bør det være umuligt for uautoriseret personale at få adgang til personlige eller systemkritiske data Eksempler på sikkerhedskontrol kan findes i OWASP
19.3	Udtrækning af krypteringsnøgler	M11	Der skal udføres sikkerhedskontrol i forbindelse med lagring af krypteringsnøgler, dvs. anvendelse af sikkerhedsmoduler
20.1	Ulovlig/uautoriseret ændring af køretøjets elektroniske ID	M7	Teknikker til og udformning af adgangskontrol skal anvendes til beskyttelse af systemdata/-kode. Eksempler på sikkerhedskontrol kan findes i OWASP
20.2	Identitetsbedrageri, f.eks. når en bruger ønsker at vise en anden identitet ved kommunikation med vejafgiftssystemer, backend-servere hos fabrikanten		
20.3	Handlinger, der foretages for at omgå overvågningssystemer (f.eks. hacking/ manipulation/blokering af meddelelser såsom ODR Tracker data, eller antal kørsler)	M7	Teknikker til og udformning af adgangskontrol skal anvendes til beskyttelse af systemdata/-kode. Eksempler på sikkerhedskontrol kan findes i OWASP. Datamanipulationsangreb på sensorer eller overførte data kan afbødes ved at forbinde data fra forskellige informationskilder
20.4	Datamanipulation med henblik på at forfalske kørselsdata (f.eks. kilometerstand, hastighed, vejvisning mm.)		
20.5	Uautoriserede ændringer af systemdiagnosedata		
21.1	Uautoriseret sletning/manipulation af systemhændelseslog	M7	Teknikker til og udformning af adgangskontrol skal anvendes til beskyttelse af systemdata/-kode. Eksempler på sikkerhedskontrol kan findes i OWASP.
22.2	Introduktion af skadelig software eller ondsindet softwareaktivitet	M7	Teknikker til og udformning af adgangskontrol skal anvendes til beskyttelse af systemdata/-kode. Eksempler på sikkerhedskontrol kan findes i OWASP.
23.1	Forfalskning af software til køretøjskontrolsystemer eller informationssystemer		

Tabel A1 reference	Trusler vedrørende "potentielle mål for eller motiver til et angreb"	Ref.	Modforanstaltning
24.1	Denial of Service, der f.eks. kan udløses på det interne netværk ved at oversvømme en CAN-bus eller ved at fremprovokere fejl på en ECU via et højt antal beskeder	M13	Der skal anvendes foranstaltninger, der gør det muligt at opdage og rette op på et Denial of Service-angreb
25.1	Uautoriseret adgang med henblik på forfalskning af konfigurationsparametre for nøglefunktioner i køretøjet, som f.eks. bremsedata, grænseværdi for udløsning af airbag osv.	M7	Teknikker til og udformning af adgangskontrol skal anvendes til beskyttelse af systemdata/-kode. Eksempler på sikkerhedskontrol kan findes i OWASP
25.2	Uautoriseret adgang med henblik på forfalskning af ladeparametre, som f.eks. ladespænding, ladeeffekt, batteritemperatur osv.		

6. Modforanstaltning vedrørende "potentielle sårbarheder, som kan udnyttes, hvis de ikke er tilstrækkeligt beskyttede eller forstærkede"

Modforanstaltninger mod trusler, der vedrører "potentielle sårbarheder, som kan udnyttes, hvis de ikke er tilstrækkeligt beskyttede eller hærdede" er anført i tabel B6.

Tabel B6

Modforanstaltninger mod trusler, der vedrører "potentielle sårbarheder, som kan udnyttes, hvis de ikke er tilstrækkeligt beskyttede eller hærdede"

Tabel A1 reference	Trusler vedrørende "potentielle sårbarheder, som kan udnyttes, hvis de ikke er tilstrækkeligt beskyttede eller hærdede"	Ref.	Modforanstaltning
26.1	En kombination af kortvarige krypteringsnøgler og en lang gyldighedsperiode gør det muligt for angriberen at bryde krypteringen	M23	Bedste praksis for cybersikkerhed for udvikling af software og hardware skal følges
26.2	Utilstrækkelig brug af kryptografiske algoritmer til beskyttelse af følsomme systemer		
26.3	Anvendelse af forældede kryptografiske algoritmer		
27.1	Hardware eller software, der er designet til at muliggøre et angreb eller ikke opfylder konstruktionskriterierne for at standse et angreb	M23	Bedste praksis for cybersikkerhed for udvikling af software og hardware skal følges
28.1	Tilstedeværelsen af softwarefejl kan være et grundlag for en potentiel udnyttelse af sårbarheder. Dette gælder især, hvis softwaren ikke er blevet testet for at kontrollere, at den ikke er behæftet med kendt dårlig kode/fejl, således at risikoen for tilstedeværelsen af sådanne reduceres	M23	Bedste praksis for cybersikkerhed for udvikling af software og hardware skal følges. Prøvning af cybersikkerhed med passende dækning

Tabel A1 reference	Trusler vedrørende "potentielle sårbarheder, som kan udnyttes, hvis de ikke er tilstrækkeligt beskyttede eller hærdede"	Ref.	Modforanstaltning
28.2	Brug af elementer fra udviklingsfasen (f.eks. fejlfindingsporte, JTAG-porte, mikroprocessorer, udviklingscertifikater, udviklingspasswords osv.) kan give en angriber adgang til ECU'er eller større privilegier		
29.1	Overflødige åbne internetporte som giver adgang til netværkssystemer		
29.2	Omgåelse af netværksadskillelse med henblik på at opnå kontrol. Et specifikt eksempel herpå er brugen af ubeskyttede gateways eller adgangspunkter (f.eks. gateways mellem lastbil og påhængskøretøj) for at omgå beskyttelse og få adgang til andre netværkssegmenter med henblik på at udføre ondsindede handlinger, som f.eks. afsendelse af vilkårlige CAN-bus-beskeder	M23	Bedste praksis for cybersikkerhed for udvikling af software og hardware skal følges. Bedste praksis for systemudformning og systemintegration skal følges

7. Modforanstaltninger vedrørende "datatab/databrud fra køretøjer"

Modforanstaltninger mod trusler, der vedrører "datatab/databrud fra køretøjer" er opført i tabel B7.

Tabel B7

Modforanstaltninger mod trusler, der vedrører "datatab/databrud fra køretøjer"

Tabel A1 reference	Trusler vedrørende "datatab/databrud fra køretøjer"	Ref.	Modforanstaltning
31.1	Informationsbrud. Personlige data kan lækkes ved ejer- eller brugerskift (dvs. bilen sælges eller bruges som udlejningsbil med nye lejere)	M24	Bedste praksis for beskyttelse af dataintegritet og fortrolighed skal følges i forbindelse med lagring af personoplysninger.

8. Modforanstaltninger vedrørende "fysisk manipulation af systemer for at muliggøre angreb"

Modforanstaltninger mod trusler, der vedrører "fysisk manipulation af systemer for at muliggøre angreb" er opført i tabel B8.

Tabel B8

Modforanstaltninger mod trusler, der vedrører "fysisk manipulation af systemer for at muliggøre angreb"

Tabel A1 reference	Trusler vedrørende "fysisk manipulation af systemer for at muliggøre angreb"	Ref.	Modforanstaltning
32.1	Manipulation af OEM-hardware, dvs. uautoriseret hardware, der tilføjes til køretøjet for at muliggøre "man-in-the-middle"-angreb	M9	Der skal anvendes foranstaltninger til forebyggelse og opdagelse af uautoriseret adgang

DEL C

Modforanstaltninger vedrørende trusler uden for køretøjet

1. Modforanstaltninger vedrørende "backend-servere"

Modforanstaltninger mod trusler, der vedrører "backend-servere" er opført i tabel C1.

Tabel C1

Modforanstaltninger mod trusler, der vedrører "backend-servere"

Tabel A1 reference	Trusler vedrørende "backend-servere"	Ref.	Modforanstaltning
1.1 & 3.1	Misbrug af privilegier blandt ansatte (insiderangreb)	M1	Der skal udføres sikkerhedskontrol på backend-systemer for at forhindre insiderangreb
1.2 & 3.3	Uautoriseret internetadgang til serveren (f.eks. via bagdøre, sikkerhedshuller i systemsoftware, SQL-angreb eller andre midler)	M2	Der skal udføres sikkerhedskontrol på backend-systemer for at forhindre uautoriseret adgang. Eksempler på sikkerhedskontrol kan findes i OWASP
1.3 & 3.4	Uautoriseret fysisk adgang til serveren (f.eks. vha. USB-nøgler eller andre medier, der er forbundet med serveren)	M8	Gennem systemdesign og adgangskontrol bør det være umuligt for uautoriseret personale at få adgang til personlige eller systemkritiske data
2.1	Angreb på backend-serveren stopper driften af serveren, f.eks. kan angrebet forhindre serveren i at interagere med køretøjer og levere de nødvendige tjenester	M3	Der skal udføres sikkerhedskontrol på backend-systemer. I tilfælde, hvor backend-servere er af afgørende betydning for leveringen af tjenester, eksisterer der backup-procedurer i tilfælde af systemnedbrud. Eksempler på sikkerhedskontrol kan findes i OWASP
3.2	Tab af oplysninger i skyen. Følsomme data kan gå tabt på grund af angreb eller ulykker, når data lagres af tredjepartsudbydere af cloudtjenester	M4	Der skal anvendes sikkerhedskontroller for at minimere risici i forbindelse med cloudcomputing. Eksempler på sikkerhedskontrol kan findes i OWASP og NCSC's retningslinjer for cloudcomputing
3.5	Informationsbrud via utilsigtet udveksling af data (f.eks. administratorfejl, lagring af data på servere i garager)	M5	Der skal udføres sikkerhedskontrol på backend-systemer for at forhindre databrud. Eksempler på sikkerhedskontrol kan findes i OWASP

2. Modforanstaltninger vedrørende "utilsigtede menneskelige handlinger"

Modforanstaltninger mod trusler, der vedrører "utilsigtede menneskelige handlinger" er opført i tabel C2.

Tabel C2

Modforanstaltninger mod trusler, der vedrører "utilsigtede menneskelige handlinger"

Tabel A1 reference	Trusler vedrørende "utilsigtede menneskelige handlinger"	Ref.	Modforanstaltning
15.1	Et uskyldigt offer (f.eks. ejer, bruger eller vedligeholdelsesingeniør) bliver narret til at foretage en handling og utilsigtet uploade malware eller muliggøre et angreb	M18	Der skal gennemføres foranstaltninger, der definerer og kontrollerer brugerroller og adgangsrettigheder, baseret på princippet om mindst mulig adgang
15.2	De definerede sikkerhedsprocedurer bliver ikke fulgt	M19	Organisationerne skal sørge for, at der er defineret sikkerhedsprocedurer, og at disse bliver fulgt, herunder registrering af handlinger og adgang forbundet med forvaltning af sikkerhedsfunktioner

3. Modforanstaltninger vedrørende "fysisk tab af data"

Modforanstaltninger mod trusler, der vedrører "fysisk tab af data" er opført i tabel C3.

Tabel C3

Modforanstaltninger mod trusler, der vedrører "fysisk tab af data"

Tabel A1 reference	Trusler vedrørende "fysisk tab af data"	Ref.	Modforanstaltning
30.1	Skade forvoldt af tredjemand. Følsomme data kan gå tabt eller blive kompromitteret grund af fysiske skader i tilfælde af færdselsuheld eller tyveri	M24	Bedste praksis for beskyttelse af dataintegritet og fortrolighed skal følges i forbindelse med lagring af personoplysninger. Eksempler på sikkerhedskontrol kan findes i ISO/SC27/WG5
30.2	Tab i forbindelse med DRM-konflikter (forvaltning af digitale rettigheder). Brugerdata kan blive slettet på grund af DRM-fejl		
30.3	(Integriteten af) følsomme data kan gå tabt på grund af slidte IT-komponenter, hvilket kan forårsage potentielle følgevirkninger (f.eks. i forbindelse med ændring af nøgle)		