Dokumentnummer
2292800

Dato
15. september 2026

Direkte
+45 36 13 16 30

CVR nr: 29 89 65 69
EAN nr: 5798000016798

Notat vedr. risikovurdering af elbusser og elbiler vedr. cybersikkerhed og datasikkerhed

1 Hovedkonklusioner

Den stigende anvendelse af softwaredefinerede og opkoblede elbusser og elbiler medfører nye sårbarheder og dermed potentielt nye cybersikkerheds- og datarisici. Problemstillingen har været genstand for stor faglig- og mediemæssig interesse. På baggrund af spørgsmål om især kinesiske busproducenters datahåndtering bad Movia i 2025 Styrelsen for Samfundssikkerhed (SAMSIK) om en vurdering af risiciene. SAMSIK svarede, at man ikke kendte til konkrete trusler fra kinesiske elbusser, men peger i sit svar på en række generelle, kendte cybersikkerhedstrusler, og opfordrede Movia til at afdække risici ved at gennemføre en risikovurdering af anvendelse af elbusser. Movia har efterfølgende bedt EY om at gennemføre en samlet risikovurdering.

Hovedkonklusionen er, at cybersikkerheds- og data risici er reelle men styrbare. Der er ikke grundlag for at konkludere, at asiatiske producenter generelt har et lavere cybersikkerhedsniveau end øvrige producenter. Risiciene knytter sig i stedet især til fjernadgang, softwareopdateringer, avancerede førerassistentsystemer (ADAS) og andre digitale afhængigheder og bør håndteres gennem klare krav, gennemsigtighed og beredskab.

Næste skridt er at omsætte risikovurderingen til konkrete kontraktkrav og styringsmekanismer i Movias eksisterende og kommende udbud og kontrakter. Fokus er på dokumentation, adgang til information, hændelsesunderretning og en risikobaseret eskalation, så Movia kan håndtere forhøjede eller kritiske situationer uden at overtage operatørernes ansvar.

2 Baggrund

Movia varetager den kollektive bustrafik i Østdanmark (undtagen Bornholm) gennem kontrakter med selvstændige operatører, der ejer og driver busserne. I takt med den grønne omstilling anvendes i stigende grad elbusser og elbiler, som i dag er softwaredefinerede og opkoblede via digitale systemer og fjernforbindelser.

Særligt ADAS, fjernovervågning og trådløse softwareopdateringer (”over-the-air”) medfører nye digitale afhængigheder. Disse teknologier giver driftsmæssige og sikkerhedsmæssige fordele, men betyder samtidig, at:

- køretøjers funktion og tilgængelighed kan påvirkes via eksterne systemer,
- beslutninger og handlinger kan udføres uden fysisk adgang til køretøjet,
- digitale hændelser potentielt kan påvirke mange køretøjer samtidigt.

Den danske myndighedsvurdering af truslen mod transportsektoren peger på et forhøjet cybertrusselsniveau, herunder en meget høj trussel fra cyberspionage. Det betyder ikke, at hvert enkelt køretøj eller hver rute skal betragtes som kritisk, men det understøtter, at Movia og operatørerne løbende bør opretholde et grundlæggende beredskab.

På den baggrund har Movia igangsat en risikovurdering af cybersikkerhed og fjernadgang for elbusser og elbiler anvendt i Movias trafik.

3 Formål med risikovurderingen

Formålet med risikovurderingen er:

- at skabe overblik over cybersikkerhedsrisici forbundet med moderne elbusser og elbiler,
- at vurdere, om gældende lovgivning og standarder giver et tilstrækkeligt grundlag for at håndtere disse risici,
- at belyse, hvordan digitale hændelser kan få betydning for drift, sikkerhed og tillid, også selvom Movia ikke ejer eller driver køretøjerne,
- og at identificere realistiske og proportionale styrings- og kontraktmæssige greb, som Movia kan anvende over for operatører og leverandører.

Risikovurderingen har ikke til formål at teste køretøjer teknisk eller at overtage operatørernes ansvar, men derimod at sikre forudsigelig håndtering af nye risici i den kollektive trafik.

4 Omfang og afgrænsning

Risikovurderingen dækker:

4.1 Elbusser i den faste rutekørsel

- Elbusser, der anvendes af Movias operatører i Movias dækningsområde, herunder modeller med og uden ADAS (avancerede førerassistentsystemer) og trådløse opdateringer.
- Vurderingen omfatter de busproducenter, der i dag leverer elbusser til Movias operatører: Yutong, BYD, MAN, Ebusco, Volvo, Golden Dragon, Mercedes-Benz/Daimler Buses og VDL.
- Fokus er på cybersikkerhed, fjernadgang og systemiske risici, ikke på køreegenskaber eller traditionel trafiksikkerhed.

Tabellen nedenfor viser antallet af idriftsatte busser pr. producent. Tallene omfatter busser i drift og ikke reservebusser.

Producent	Idriftsatte busser
Yutong	299
BYD	259
MAN	67
Ebusco	49
Volvo	29
Golden Dragon	27
Daimler / Mercedes-Benz	26
VDL	23
I alt	779

Trafikselskabet Movia Hanne Varmings Plads 4, 2500 Valby – DK +45 36 13 14 00 movia@moviatrafik.dk

4.2 Elbiler i Flextrafik

- Elbiler anvendt eller egnet til brug i Movias behovsstyrede transport (Flextrafik).
- Analysen omfatter to elbilplatforme: BYD Seal U og Tesla Model 3/Model Y.

Opgavebeskrivelsen forudsætter analyse af to elbilmodeller; én produceret af en kinesisk producent og én produceret af en europæisk producent. BYD Seal U indgår som den kinesiske referenceplatform og dækker dermed det kinesiske element.

I stedet for en europæisk model er Tesla valgt som analyseenhed, da producenten repræsenterer en højt softwaredefineret og opkoblet elbilarkitektur med omfattende anvendelse af ADAS, fjernadgang og trådløse softwareopdateringer, og da modellerne er udbredte. Det udgør en bevidst afgrænsning i forhold til opgavebeskrivelsens forudsætning om en europæisk model. Analysen giver et konservativt og risikoorienteret billede af de cybersikkerheds- og ADAS-relaterede problemstillinger, der er relevante for Flextrafik, og skal læses som indikativ.

5 Metode

Undersøgelsen er gennemført som en skrivebordsanalyse og består af to hovedelementer:

Vurdering af producenternes strukturelle cybersikkerhed:

- baseret på spørgeskemaer og tilgængelig dokumentation,
- tilpasset internationale standarder og regulering.

Overordnet risikovurdering:

- ser på, hvordan teknisk plausible hændelser kan få driftsmæssige og samfundsmæssige konsekvenser,
- med fokus på eskalation, afhængigheder og styring – ikke sandsynlighedsberegninger.

Der er ikke foretaget tekniske tests, inspektioner eller revisioner af køretøjerne. Vurderingen af elbiler i Flextrafik er indikativ og udgør ikke en fuldstændig sammenlignende gennemgang af elbilmarkedet.

6 Lovgivningsmæssigt grundlag

Cybersikkerhed for moderne køretøjer bygger på en kombination af bindende regulering, internationale standarder og regler om data- og cybersikkerhed:

- **UNECE-regulering R155 –** krav til producenternes cybersikkerhedsledelse (CSMS),
- **UNECE-regulering R156 –** krav til styring af softwareopdateringer (SUMS),
- **ISO/SAE 21434 –** international standard for cybersikkerhed i køretøjer,
- **ISO 24089 –** international standard for softwareopdatering i køretøjer,
- **GDPR –** databeskyttelsesforordningen for håndtering af persondata.
- **NIS2-loven**, hvor Movia, operatører eller leverandører er omfattet, særligt i forhold til governance, risikostyring, leverandørstyring og hændelseshåndtering.

For fremtidige, mere automatiserede køretøjer er desuden UNECE-regulering R157 (typegodkendelse af automatiserede kørefunktioner) og ISO 26262 (funktionel sikkerhed) relevante.

Risikovurderingen viser, at dette regelsæt overordnet er tilstrækkeligt, forudsat at:

- kravene faktisk efterleves,

Trafikselskabet Movia Hanne Varmings Plads 4, 2500 Valby – DK +45 36 13 14 00 movia@moviatrafik.dk

- styringen fortsætter, efter køretøjer er taget i brug,
- og at der er gennemsigtighed og dokumentation.

Lovgivningen kan således håndtere de identificerede risici i princippet – men effekten afhænger af implementering og styring.

7 Overordnede resultater

Undersøgelsen viser markante forskelle mellem producenterne i, hvor modent og dokumenteret deres arbejde med cybersikkerhed er. Følgende områder er vurderet:

- **Styring og ansvar (governance):** om producenten har et ledelsessystem (CSMS) og klart ansvar for cybersikkerhed i hele køretøjets levetid.
- **Risikoanalyse:** om trusler og sårbarheder identificeres og vurderes systematisk (TARA).
- **Systemarkitektur:** om kritiske systemer er adskilt fra mindre kritiske, så fejl ikke spreder sig.
- **Styring af softwareopdateringer:** om opdateringer leveres kontrolleret og ægthedssikret og kan rulles tilbage ved fejl.
- **Test og validering:** om sikkerhedsforanstaltninger faktisk afprøves og virker som tilsigtet.
- **Håndtering af sikkerhedshændelser:** om producenten kan opdage, reagere på og lære af hændelser.

Samlet billede:

- Flere producenter har høj modenhed og dokumenterede processer.
- Ældre busplatforme uden moderne cybersikkerhedsrammer giver lavere gennemsigtighed og kontrol.
- Høj producentmodenhed reducerer risiko, men eliminerer den ikke.

Nedenstående tabel viser dokumenteret alignment med de vurderede kravområder. Tabellen er ikke en direkte risikovurdering og er ikke en formel juridisk certificeringsvurdering.

VDL falder væsentligt ud på dokumenterbarhed, hvilket kan henføres til, at de anvendte modeller er væsentligt ældre, leveret før UN R155 og UN R156 trådte i kraft, og ikke er udstyret med trådløse opdateringer. Den manglende OTA-funktionalitet reducerer risikoen for fjernbaseret, flådeomfattende softwarekompromittering, men den lave dokumenterbarhed indebærer samtidig mindre gennemsigtighed, livscyklusstyring og auditmulighed. De nye platforme fra VDL forventes at bringe sikkerheden op på niveau er de øvrige leverandører.

Område	VDL	EBUSCO	BYD	Golden Dragon	Yutong	Daimler	MAN	Tesla	BYD Seal U
Styring	10%	90%	100%	86%	100%	86%	100%	100%	100%
Risikoanalyse	0%	95%	100%	100%	95%	90%	85%	100%	100%
Arkitektur	56%	100%	100%	100%	100%	78%	100%	100%	100%
Softwareopdateringer	40%	60%	90%	90%	100%	70%	90%	100%	90%
Validering	8%	100%	100%	92%	100%	92%	100%	100%	100%
Hændelseshåndtering	14%	43%	79%	86%	93%	64%	86%	100%	79%

På det foreliggende dokumentationsgrundlag er der ikke grundlag for at konkludere generelle, systematiske forskelle i cybersikkerhedsniveauet mellem de undersøgte asiatiske producenter og øvrige producenter. Vurderingen bør dog læses som model- og dokumentationsafhængig.

Volvo 7900E indgår i flådeopgørelsen med 29 busser. Da der ikke foreligger tilstrækkeligt spørgeskema-

Trafikselskabet Movia Hanne Varmings Plads 4, 2500 Valby – DK +45 36 13 14 00 movia@moviatrafik.dk

eller dokumentationsgrundlag for Volvo, er Volvo ikke tildelt en sammenlignende score. Dette skal betragtes som et dokumentationshul og ikke som en negativ cybersikkerhedsvurdering.

8 Centrale risici identificeret i analysen

8.1 Fjernadgang og afhængighed af interne aktører

Moderne elbusser og elbiler kræver legitim fjernadgang for bl.a. vedligehold, fejlfinding og softwareopdateringer. Samtidig betyder det, at:

- handlinger kan udføres uden fysisk adgang,
- det kan være vanskeligt at skelne mellem fejl, misbrug og legitime handlinger,
- og at konsekvenser hurtigt kan eskalere, hvis flere køretøjer påvirkes.

Risikoen ligger ikke primært i hacking udefra, men i den strukturelle afhængighed af adgang, der er teknisk legitim – herunder hos producenter og leverandører.

8.2 Nye risici fra ADAS (avancerede førerassistentsystemer)

Avancerede førerassistentsystemer ændrer risikobilledet:

- Fejl kan opstå gradvist og være svære at opdage.
- Softwareændringer kan påvirke kørselsmønstre og assistancefunktioner.
- Centraliserede systemer kan betyde, at fejl rammer mange køretøjer samtidigt.

Konsekvensen kan være driftsforstyrrelser, tvivl om sikkerhed og pres på både operatøren og Movia for hurtige beslutninger uden fuldt overblik. På reguleringssiden er UNECE R157 den første internationale ramme for typegodkendelse af automatiserede kørefunktioner og vil i stigende grad omfatte netop de funktioner, hvor en kompromittering har de mest direkte konsekvenser.

8.3 Persondata og ikke-producentinstallerede systemer (ikke-OEM-systemer)

Ud over selve køretøjet behandles persondata i en række systemer, fx kameraer til passagertælling og videoovervågning (CCTV), billettering (Basiskort), GPS/telemetri og diagnostik. Disse data udgør sjældent en direkte sikkerhedsrisiko, men er relevante i forhold til GDPR, fortrolighed og tillid. Ikke-OEM-systemer monteret af operatører eller leverandører kan desuden udvide angrebsfladen, hvis de ikke er adskilt fra sikkerhedskritiske køretøjssystemer. Ansvaret for disse systemer påhviler typisk operatøren eller systemejeren, mens Movia har ansvaret for Movia-ejede systemer som Basiskort.

8.4 Ladeinfrastruktur

Ladeinfrastruktur introducerer yderligere digitale grænseflader uden for selve køretøjet. Veladskilte arkitekturer bør forhindre direkte påvirkning af køretøjets styring, men kompromitterede eller utilgængelige ladesystemer kan føre til omfattende driftsforstyrrelser. Den dominerende risiko er derfor tilgængelighed og kontinuitet snarere end direkte fjernstyring af køretøjerne. Movia bør basere sig på standardbaseret sikring (fx IEC 62443 eller tilsvarende), klar ejerfordeling af fysisk og netværksmæssig sikkerhed på depoter, definerede procedurer for hændelseshåndtering samt nødplaner ved ladingsrelaterede afbrydelser.

9 Risikoniveauer og håndtering

For at sikre forudsigelig og proportional håndtering anvender risikovurderingen en eskalationsmodel med

Trafikselskabet Movia Hanne Varmings Plads 4, 2500 Valby – DK +45 36 13 14 00 movia@moviatrafik.dk

tre risikoniveauer:

- **Normalt niveau:** almindelig drift, almindelig kontraktstyring og overvågning.
- **Forhøjet niveau:** fx ved varsler fra myndigheder eller reduceret gennemsigtighed – skærpet opmærksomhed, bedre informationsadgang og beredskab.
- **Kritisk niveau:** ved bekræftede hændelser eller myndighedspåbud – midlertidige, forholdsmæssige tiltag med fokus på sikkerhed og kontinuitet.

Et konkret eksempel på et trinvist tiltag er styring af opkobling: operatører kan stilles krav om at anvende europæiske SIM-kort, der kan deaktiveres helt eller delvist – enten for det enkelte køretøj eller for hele flåden – hvis trusselsniveauet stiger.

Modellen tydeliggør, hvornår og hvordan Movia forventes at reagere, uden at Movia overtager operatørernes ansvar.

10 Movias rolle og ansvar

Movia ejer ikke køretøjerne og driver ikke OEM- eller operatørsystemerne. Movia har derimod som trafikselskab og kontraktmyndighed ansvar for at stille klare, proportionale krav, der understøtter sikker og stabil kollektiv trafik. Risikovurderingen peger på, at Movias vigtigste styringsgreb er:

- klar kontraktlig rollefordeling mellem Movia og operatørerne,
- gennemsigtighed i fjernadgang og hændelser,
- foruddefinerede beslutnings- og eskalationsmekanismer,
- fokus på hurtig afgrænsning frem for teknisk skyldplacering.

Til understøttelse heraf beskriver risikovurderingen en række mitigerende tiltag og konkrete, standardbaserede kontraktkrav til både nuværende og fremtidige udbud og kontrakter.

De konkrete kontraktkrav kan bl.a. omfatte:

- **Standardbaseret baseline:** overholdelse af UN R155/R156, hvor relevant, samt ISO/SAE 21434 og ISO 24089 eller tilsvarende dokumenteret praksis.
- **Proportional informationssikkerhed:** passende informationssikkerhedsforanstaltninger for operatørstyrede IT-systemer og backend-miljøer, samt relevant dokumentation fra underleverandører, der behandler eller har privilegeret adgang til data.
- **NIS2 og governance:** krav om, at NIS2-relevante forpligtelser afspejles i operatørens governance, risikostyring, leverandørstyring og hændelseshåndtering, hvor operatøren eller leverandøren er omfattet.
- **Opkoblede funktioner og deaktivering:** krav om overblik over OTA-opdateringer, fjernadgang og automatisk dataoverførsel, samt mulighed for vurdering, eskalation og, hvor lovligt og teknisk muligt, hel eller delvis deaktivering efter konkret risiko- og driftsvurdering.
- **Styring af softwareopdateringer:** krav om, at opdateringer håndteres via OEM'ens dokumenterede processer, herunder UN R156 og, hvor relevant, ISO 24089 eller tilsvarende dokumentation.
- **Hændelsesunderretning og eskalation:** underretning uden ugrundet ophold ved kendte eller mistænkte hændelser, relevante myndighedsvarsler og OEM- eller leverandørmeddelelser, der kan påvirke sikkerhed, drift, data eller offentlig tillid.
- **Evidens og audit:** dokumentation som led i almindelig kontraktopfølgning og mulighed for proportional tredjepartsverifikation ved begrundet mistanke eller væsentlig hændelse.
- ***Ældre køretøjer uden for R155/R156:*** proportional minimumsbaseline med dokumentation for grænseflader, adgangskontrol og logning af værksteds- og diagnoseadgang.

Trafikselskabet Movia Hanne Varmings Plads 4, 2500 Valby – DK +45 36 13 14 00 movia@moviatrafik.dk

- **Ikke-OEM-systemer:** sikker konfiguration, vedligeholdelse, opdatering og segmentering fra sikkerhedskritiske køretøjssystemer.
- **Databeskyttelse:** GDPR-efterlevelse og begrænsning af dataoverførsel uden for EU/EØS uden Movias godkendelse.
- **Ladeinfrastruktur:** relevant og proportional anvendelse af IEC 62443 eller tilsvarende principper, særligt hvor ladeinfrastrukturen har væsentlig betydning for driftskontinuiteten.

11 Samlet konklusion

Risikovurderingen viser, at:

- cybersikkerhed i moderne elbusser og elbiler er en reel, men styrbar risiko,
- lovgivning og standarder er i hovedtræk tilstrækkelige,
- høj producentmodenhed er i fokus og nødvendig, men ikke tilstrækkelig alene,
- risikoen opstår især i samspillet mellem teknologi, organisation og ansvar.

Konklusionerne vedrørende elbiler i Flextrafik baserer sig på analyse af to elbilplatforme (BYD Seal U og Tesla) og kan derfor ikke uden videre generaliseres til alle elbiler. Analysen giver et konservativt og risikoorienteret indblik, men udgør ikke en fuldstændig markedsanalyse.

Med klare forventninger, gennemsigtighed og proaktive styringsmekanismer kan Movia fortsat understøtte innovation i den kollektive trafik uden at gå på kompromis med sikkerhed, drift og tillid.

Trafikselskabet Movia Hanne Varmings Plads 4, 2500 Valby – DK +45 36 13 14 00 movia@moviatrafik.dk