Tekna –
Teknisk-naturvitenskapelig forening
Postboks 2312 Solli
0201 Oslo

www.tekna.no
Org.nr 971 420 782
post@tekna.no
+47 22 94 75 00

Samferdselsdepartementet

Vår ref.:
TPL / MKF

Dato:
16. november 2026

Teknas høringssvar om risikoreduserende tiltak i bussanskaffelser – endring i nullutslippsforskriften og forslag til veiledning

Tekna er fagforeningen for over 122 000 naturvitere og teknologer. Våre medlemmer har høyere utdanning på master- og doktorgradsnivå og representerer viktige kunnskapsmiljøer i Norge.

Tekna støtter målet om å redusere leverandøravhengighet og konsentrasjonsrisiko i bussflåten. Busser er en sentral ressurs i den sivile og militære beredskapen, og det er riktig at departementet tar risikoen ved en ensidig sammensatt bussflåte på alvor.

Samtidig slår departementet selv fast at sårbarhetene ikke er knyttet til drivlinjen, men til moderne, oppkoblede kjøretøy generelt. En diesel- eller biogassbuss kan ha de samme avhengighetene til programvare, fjernaksess, digitale oppdateringer og leverandørstyrte systemer som en elektrisk buss. Å åpne for en annen drivlinje løser derfor ikke i seg selv sikkerhetsutfordringen som departementet beskriver.

Departementet påpeker også at dagens kunnskapsgrunnlag gjør det krevende å vurdere hvilke kjøretøytekniske tiltak som er mulige og hensiktsmessige. Statens vegvesen har derfor fått i oppdrag å bygge mer kunnskap om blant annet hvilke data som sendes fra bussene, hvilke sårbarheter dette skaper og hvilke tiltak som kan begrense muligheten for uønsket påvirkning.

Dette vil gi myndighetene et bedre grunnlag for å vurdere hvilke tiltak som faktisk reduserer risikoen, og om et unntak fra nullutslippskravet er nødvendig eller treffsikkert. Kunnskapsprosjektet vil også gi et bedre grunnlag for å utforme teknologinøytrale sikkerhetskrav til fremtidige busser, uavhengig av produsentland, digital verdikjede og drivlinje.

Tekna mener at det foreslåtte unntaket fra nullutslippskravet bør settes på vent til Statens vegvesen har avsluttet sitt pågående kunnskapsprosjekt om kjøretøytekniske tiltak knyttet til busser.

Sårbarheten ligger i den digitale arkitekturen

Ruters tekniske sikkerhetsundersøkelse illustrerer problemstillingen. Den testede Yutong-bussen hadde mulighet for selvstendige programvareoppdateringer og digital tilgang til styringssystemer for batteri og kraftforsyning via mobilnettet. Den testede VDL-bussen hadde ikke tilsvarende mulighet for selvstendige fjernoppdateringer. Ruter understreker selv at problemstillingen knytter seg til teknologien som gjør bussene oppkoblet, ikke til produsent eller opprinnelsesland.

Tekna støtter departementets påpekning om at sårbarhet ikke er knyttet til drivlinjen, og vi vil vise til ITS Norway tre punkter som gjelder moderne kjøretøy uavhengig av produksjonsland:

- Kjøretøy samler inn og sender data om blant annet posisjon og status. Operatøren må vite hvilke data som samles inn, hvem som mottar dem og hva de brukes til.

- Stadig flere kjøretøyfunksjoner styres av programvare. Med førerstøttesystemer og andre digitale funksjoner blir det derfor stadig viktigere å vite hvem som har den faktiske kontrollen over kjøretøyet, og om nødvendig funksjonalitet kan opprettholdes dersom forbindelsen til produsenten brytes.

- Programvareoppdateringer over nettet, såkalte Over-the-Air-oppdatering (OTA), styres i stor grad av produsenten. Det kan redusere operatørens innsyn i hvilke endringer som gjøres i kjøretøyets programvare og funksjonalitet.

Tekna vil i tillegg påpeke at det også er viktig å ha kontroll over når slike oppdateringer gjennomføres. For busser som skal være i kontinuerlig drift kan det få alvorlige konsekvenser dersom en programvareoppdatering skjer på et tidspunkt som gjør kjøretøyet midlertidig utilgjengelig eller fører til driftsavbrudd.

TRASIFORA, ITS Norways forum for nasjonal transportsikkerhet og samfunnsrisiko, har siden 2025 samlet offentlige og private aktører for å kartlegge risiko knyttet til programvaredefinerte kjøretøy, datainnsamling, tilsyn med oppkoblede kjøretøy og transportberedskap. Forumet har blant annet reist spørsmålet om digitale oppdateringsplattformer for kjøretøy bør regnes som kritisk infrastruktur.

Erfaringen fra TRASIFORA er at problemstillingen blir for snever dersom debatten reduseres til én teknologi eller kjøretøy fra ett bestemt land.

Sårbarhetene er knyttet til hele den digitale verdikjeden og til hvem som har tilgang til, kontroll over og ansvar for de digitale systemene. Forumet har også pekt på at det i dag er uklart hvilken myndighet som har ansvar for å følge opp sårbarheter i oppkoblede kjøretøy.

Diversifisering må kombineres med tekniske sikkerhetskrav

Tekna mener konsentrasjonsrisikoen er reell, og at diversifisering er et riktig tiltak. Men flere leverandører gir ikke nødvendigvis større sikkerhet dersom de samme digitale avhengighetene består.

Diversifisering bør derfor kombineres med teknologinøytrale krav til kontroll over programvare, dataflyt, fjernaksess og digitale oppdateringer. Slike krav bør gjelde uavhengig av hvilket land kjøretøyet er produsert i.

Ruters siste bussanskaffelse viser at det allerede er mulig å stille mer konkrete krav til digital kontroll. Ruter krever blant annet at fjernoppdateringer, fjernaksess og automatisk dataoverføring skal kunne slås av på kort varsel, uten at bussen blir ubrukelig. Leverandørene må også redegjøre for hvilke data som samles inn, hvor de lagres, hvem som får tilgang til dem og hvilke underleverandører eller skytjenester som er inne i bildet.

Tekna mener departementets veiledning bør ta utgangspunkt i denne typen krav**.** Offentlige oppdragsgivere bør vite hvem som har tilgang til kjøretøyet, hvilke eksterne tjenester det er avhengig av, og om bussen fortsatt fungerer dersom forbindelsen til produsenten eller andre leverandører brytes.

Kravene må kunne kontrolleres i praksis, slik at det ikke bare blir noe leverandøren beskriver i tilbudet. Når kjøretøy skal inngå i samfunnets beredskap, må oppdragsgiver kunne være trygg på at funksjoner faktisk kan kobles ut, og at dataflyten stopper når den skal.

Sikkerhet og digital suverenitet må få reell vekt i offentlige anskaffelser

Tekna mener sikkerhet og digital suverenitet må vektes tyngre i offentlige anskaffelser av samfunnskritisk teknologi. Pris kan ikke være det tungtveiende kriteriet dersom det billigste alternativet samtidig gjør oss mer avhengige av leverandører utenfor Europa eller gir mindre kontroll over programvare, data og kritiske leverandørkjeder.

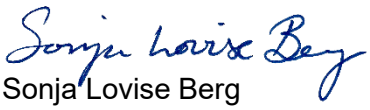
Dersom vi skal lykkes med å redusere denne avhengigheten, må vi også være villige til å investere i europeiske alternativer. På kort sikt kan det koste mer, men på lengre sikt vil dette kunne bidra til å bygge opp en europeisk

leverandørindustri. Dette vil gi oss større kontroll over teknologien og redusere sårbarhetene ved teknologien vi er avhengige av.

Etter Teknas syn må derfor offentlige innkjøp brukes mer aktivt for å stimulere det europeiske markedet. Sikkerhet, digital suverenitet og anstendige arbeidsforhold i leverandørkjeden må få reell vekt når tilbudene vurderes. Anskaffelsesregelverket og kriteriene i konkurransene må innrettes slik at oppdragsgivere faktisk kan vektlegge sikkerhet og redusert leverandøravhengighet, også når dette innebærer en høyere innkjøpspris.

Tekna bidrar gjerne i det videre arbeidet med veilederen og kravspesifikasjonene.

Med vennlig hilsen



Sonja Lovise Berg
Direktør samfunnspolitikk