DSB

Risikoanalyse av

Manipulering av satellittbaserte tidssignaler

Analyser av krisescenarioer (AKS)

Direktoratet for samfunnssikkerhet og beredskap

Utgitt av Direktoratet for samfunnssikkerhet og beredskap (DSB) 2026

Omslagsfoto: Colourbox

ISBN 978-82-7768-564-9 (PDF)

HR 2472

Grafisk produksjon: Mediehuset Andvord

Risikoanalyse av

Manipulering av satellittbaserte tidssignaler

Analyser av krisescenarioer (AKS)

Innhold

Oppsummering

Viktige samfunnsfunksjoner er i stor grad digitaliserte og i praksis avhengige av nøyaktig og synkronisert tid for å fungere. Enkle operasjoner som å logge på PC-en og å sende eposter, avhenger av flere systemer som samarbeider på basis av en felles tid. Tidssynkronisering er det som muliggjør informasjonsflyt innad i og mellom systemer, og binder det digitaliserte samfunnet sammen.

Selv om manipulering av tid (spoofing) kan påvirke folk direkte f.eks. gjennom at mobiltelefonen viser feil tid og posisjon, er det først og fremst påvirkning av kritiske samfunnsfunksjoner som får alvorlige konsekvenser for samfunnet. Funksjoner som strømforsyning, elektronisk kommunikasjon, finansielle transaksjoner og luft-, sjø-, bane- og veitransport, er alle helt avhengige av tilgang til nøyaktig tid.

I digitaliserte systemer er det snakk om små tidsvinduer for utveksling av informasjon, som et millisekund (1/1000 sekund) eller et mikrosekund (1/1 000 000 sekund). Hvis ikke avsender og mottaker har helt synkronisert tid, når ikke informasjonen fram. I og mellom digitale systemer utveksles store mengder informasjon kontinuerlig, og manglende tidssynkronisering fører til at informasjonsflyten stopper opp og funksjoner slutter å fungere.

Den mest brukte kilden til tidsangivelse er navigasjonssatellitter og i vesten er GPS dominerende tidskilde. Satellittene er utstyrte med atomklokker, som synkroniseres med universell tid UTC.

I vårt scenario blir seks ulike samfunnsfunksjoner utsatt for spoofing over en periode på flere uker.

En statlig aktør står bak den koordinerte og målrettede manipuleringen av tid til utvalgte satellittmottakere. Forfalskningen av tidssignaler er vanskelig å oppdage og får store konsekvenser.

Sårbarhet

Analysen identifiserer sju faktorer som påvirker sårbarheten for spoofing, hvorav de to første er de mest grunnleggende og den siste (redundans) er en motvekt mot de øvrige:

- **Ulike tidskilder**
  Bruk av flere tidskilder kan skape usynkronisert tid mellom datasystemer i en virksomhet og mellom virksomheter, slik at de ikke kan samhandle. Det er generelt manglende innsikt i hvordan mottak og synkronisering av tid foregår.

- **Grad av digitalisering**
  Digitalisering av funksjoner og tjenester skaper økt avhengighet av nøyaktig og synkronisert tid.

- **Avhengighet av mikrotid**
  Krav til effektivisering og hurtigere dataflyt krever oppdeling av tid i stadig mindre enheter (tidsvinduer). Mens man før kunne ha et millisekund på å utveksle data, må man nå utveksle samme mengde data på et mikrosekund. Det stiller høye krav til leveransen av tid og gir veldig små feilmarginer.

- **Distribuerte systemer med sårbare ytre ledd**
  Mange samfunnsfunksjoner krever sentralisert overvåking og styring i kontrollsentraler av

elektroniske komponenter i store geografiske områder. Utbredt bruk av GPS gjør komponentene sårbare for spoofing.

- **Åpne systemer**
  Åpne nett med mange brukere, som f.eks. internett og 5G, gir mindre grad av kontroll enn lukkede systemer.

- **Avhengighet av GPS**
  De globale GNSS-satellittsystemene tilhører i dag USA, Kina, Russland og Europa (EU). Amerikanske GPS er det klart mest brukte i vesten. Satellitter kan slås ut ved krigføring i rommet og signaler fra ett system kan forfalskes i elektronisk krigføring. Å være avhengig av kun ett satellittsystem er derfor sårbart.

- **Manglende redundans**
  I virksomheter med spesielt høye krav til nøyaktig, sikker og pålitelig tid, er ikke satellitt-basert tid gode nok tidskilder alene. De må få tid direkte fra atomklokker eller gjennom et definert NTP-nettverk med en pålitelig tidskilde. Flere tidskilder skaper redundans hvis klokkene er satt opp i riktig hierarki.

Tabellen viser hvordan vi vurderer at faktorene over påvirker sårbarheten i de seks analyserte samfunnsfunksjonene.

Funksjoner / Sårbarhetsfaktorer	Strømforsyning	Digital infrstruktur	Finansielle tjenester	Luftfart	Jernbane	Veitransport
1. Ulike tidskilder	🟡→🟢	🟡	🟡	🔴	🟢→🟡	🔴
2. Grad av digitalisering	🔴	🔴	🔴	🟡→🔴	🟢→🔴	🟡
3. Avhengighet av mikrotid	🔴	🔴	🔴	🟡→🔴	🟢→🟡	🟢
4. Distribuerte systemer	🟡	🟡	🔴	🔴	🟡	🟢→🟡
5. Åpne systemer	🟢	🟡	🟢	🟡	🟢→🟡	🔴
6. GPS-avhengighet	🔴→🟡	🟡	🟡	🔴	🟢→🟡	🔴
7. Manglende redundans	🟡→🟢	🟢	🟢	🟡	🟢	🔴

🔴 = stor grad 🟡 = moderat grad 🟢 = liten grad

En sirkel viser vurdering av dagens situasjon og to sirkler viser dagens situasjon og forventet utvikling.

Strømforsyning

Kraftsektorens sårbarhet handler i stor grad om digitalisering, avhengighet av mikrotid og bruk av satellittbasert tid i ytre ledd av systemet. Nøyaktig og synkronisert tid er helt nødvendig for å overvåke balansen i strømnettet, særlig i transmisjonsnettet. Tid hentes i stor grad fra satellitter og spoofing kan dermed skape tidsavvik som kan tolkes som fasefeil og føre til utkoblinger.

Digital infrastruktur

Elektronisk kommunikasjon er sårbar for tidsfeil på grunn av høy grad av digitalisering og avhengighet av svært nøyaktig tid. Det landsdekkende transportnettet til Telenor har imidlertid tidskilder med god redundans. Operatører som bruker GNSS-mottakere på base-stasjoner utgjør en sårbarhet både for seg selv og andre operatører i samme dekningsområde.

Finansielle tjenester

Den største sårbarheten ved tidsfeil i finansielle tjenester er høy grad av digitalisering og avhengighet av mikrotid. Norges Bank sentralt har en sikker og redundant løsning for nøyaktig tid. Avvik fra denne tiden på noen mikrosekunder fører til at andre banker avvises fra handel og oppgjør.

Luftfart

Luftfart er sårbar for tidsfeil siden flyene bruker GPS i sin kommunikasjon med kontrolltårnet, som får tid fra et internt nettverk i Avinor med atomklokker. Sårbarheten øker med innføring av satellittbaserte innflyvningsprosedyrer til erstatning for bakkebasert utstyr.

Jernbane

Jernbanen er i dag lite sårbar mot spoofing. Styring og overvåking fra trafikkstyringssentralene er i stor grad basert på mekanisk utstyr i togsporene og kommunikasjonen med togførerne skjer i et lukket mobilnett. Etter innføring av nytt digitalt signalsystem (ERTMS) de kommende årene, vil togstyringen bli langt mer avhengige av nøyaktig tid.

Veitransport

Veitransporten er sårbar for tidsfeil på grunn av bruk av satellittbasert tid både sentralt, regionalt og lokalt. Elektronisk utstyr langs veiene og i tunneler kommuniserer med vegtrafikksentralene og får tid gjennom mobilnettet. GPS brukes der det ikke er mobildekning og til koordinering av veiarbeid. Krav til nøyaktig tid vil øke fra millisekunder til mikrosekunder med innføring av «Intelligente transportsystemer».

Konsekvenser for samfunnet

De største konsekvensene for samfunnet av vellykket spoofing av flere kritiske samfunnsfunksjoner, er store økonomiske tap på grunn av feilretting og tapte inntekter, omfattende påkjenninger og uro fordi tjenester folk bruker hver dag faller bort i perioder, og frykt for å miste nasjonal kontroll over funksjoner samfunnet er helt avhengig av.

Tiltak

Det er neppe ønskelig å gjøre noe med den mest grunnleggende drivkraften til avhengighet av nøyaktig tid, nemlig digitalisering. Digitaliseringstrenden er teknologidrevet og gir store effektiviseringsgevinster. Virksomheter kan redusere avhengigheten av satellittbasert tid ved å bruke flere tidskilder i riktig konstellasjon. Myndighetene kan bidra til økt robusthet ved å sørge for enkel tilgang til pålitelig tid fra tidskilder under nasjonal kontroll.

Analyseresultatene utdypes i kapittel 7-9.

1 Hvorfor er nøyaktig tid viktig?

Digitalisering og automatisering fører til mer effektive arbeidsprosesser og forenkler hverdagen for folk flest. Dette krever deling av store mengder data. Ikke minst krever overvåkings- og styringssystemer rask flyt av data i sanntid. For å skape orden i dataflyten, må informasjonen som utveksles få et tidsstempel. Tidsstemplingen dokumenterer at alt skjer i riktig rekkefølge og til rett tid.

«Rett tid» er i denne sammenheng nøyaktig *lik tid*. Synkronisering av tid er derfor avgjørende for at alle enheter (datamaskiner, servere osv.) i et system kan kommunisere og fungere, og at ulike systemer skal fungere sammen. Presisjonen må noen ganger være ned til et mikrosekund eller 1/1 000 000 sekund.

Mange kritiske samfunnsfunksjoner er avhengig av tilgang til nøyaktig tid, f.eks. strømforsyning, elektronisk kommunikasjon, finansielle transaksjoner og luft-, sjø-, bane- og veitransport. Den mest brukte kilden til tidsangivelse er navigasjonssatellitter, som GPS og Galileo. De er utstyrte med atomklokker, som synkroniseres med universell tid UTC, dvs. standarden for fastsettelse av lokal tid over hele verden.

Signalene fra navigasjonssatellitter er svake og kan lett forstyrres av andre radiokilder som skaper interferens. Det kan være støysending (jamming), sending av falske signaler (spoofing) eller retransmisjon av et forsinket signal (meaconing). Tilsiktet interferens brukes i elektronisk krigføring og som et ikke-militært virkemiddel for å ramme kritiske samfunnsfunksjoner.[1]

Flere omfattende spoofing-hendelser er registrert de siste årene, se vedlegg 2.

Justervesenet, som ligger under Nærings- og fiskeridepartementet, har ansvar for Norges offisielle tid og vedlikehold av atomklokker i et nasjonalt laboratorium og deltar i det internasjonale samarbeidet om UTC, verdens felles tid. Nasjonal kommunikasjonsmyndighet (Nkom) har ansvar for sikkerhet og robusthet i digital infrastruktur og samarbeider med Justervesenet om å sikre pålitelig og sporbar tid.

DSB analyserer risiko for manipulering av satellittbaserte tidssignaler fordi nøyaktig tid er en felles innsatsfaktor som alle sektorer og totalforsvaret er avhengige av.[2]

Vi har formulert følgende analysespørsmål som vi forsøker å besvare i denne rapporten:

- På hvilke måter er kritiske samfunnsfunksjoner avhengige av nøyaktig tid?
- Hvilke kilder til nøyaktig tid brukes i dag?
- Hva blir konsekvensene for samfunnet av falske tidssignaler?

1 Rapport: Russland manipulerer GPS-signaler over hele verden, Over 20 skip GPS-hacket i Svartehavet

2 Parallelt med DSBs analyse, har Forsvarets forskningsinstitutt (FFI) utarbeidet en analyse om avhengigheter av satellittbaserte tjenester og Menon Economics har utført en samfunnsøkonomisk analyse av satellittbaserte PNT-tjenester.

2 Hva er nøyaktig tid og hvor kommer den fra?

2.1 Hva er «nøyaktig tid» og hvorfor er det viktig?

I digitaliserte systemer er det snakk om små tidsvinduer for utveksling av informasjon, som et millisekund (1/1000 sekund) eller et mikrosekund (1/1 000 000 sekund). Hvis ikke avsender og mottaker har helt synkronisert tid, når ikke informasjonen fram. I og mellom digitale systemer utveksles store mengder informasjon kontinuerlig, og manglende tidssynkronisering fører til at informasjonsflyten stopper opp og funksjoner slutter å fungere.

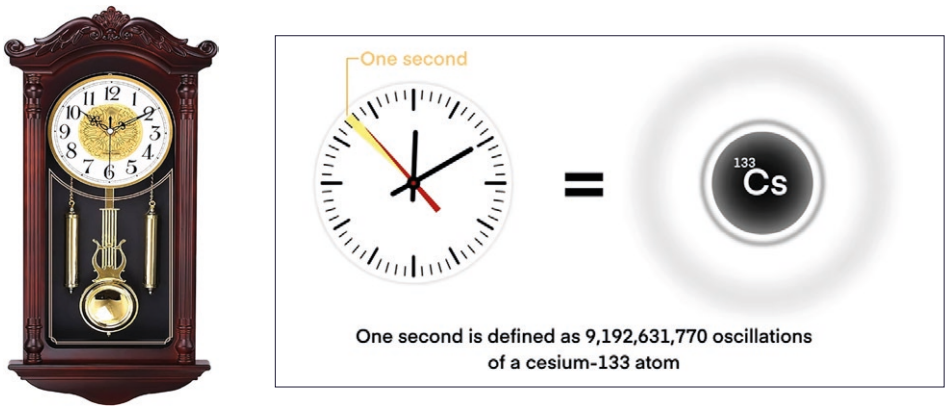
2.2 Kilder til nøyaktig tid

GNSS (Global Navigation Satellite System) er en samlebetegnelse for systemer av satellitter i bane rundt jorden[3]. De sender signaler vi bruker til posisjonering, navigasjon og tidsangivelse (PNT) ved hjelp av mottakere på bakken. Det finnes fire slike satellittsystemer i dag med global dekning: Amerikanske GPS, europeiske Galileo, kinesiske BeiDou og russiske GLONASS. GPS er den desidert mest brukte tidskilden i Norge.

En annen tidskilde er atomklokker som måler tid ved hjelp av den naturlige rytmen til atomer. Alle GNSS-satellitter inneholder en atomklokke.

Universell tid UTC er basert på synkroniserte tidsmålinger fra flere hundre atomklokker rundt om i verden, blant annet hos Justervesenet i Norge. Atomklokker og UTC kan dokumentere/bevise sikkerheten i

Figur 1: Cesium-atomet danner grunnlaget for definisjonen av ett sekund. Ett sekund er drøyt ni milliarder svingninger i et Cesium-133-atom, mens pendelen i en veggklokke svinger en gang i sekundet.



3 En viktig del av satellittsystemer er overvåkning, styring og programvareoppdateringer fra bakken.

tidsangivelse og gir derfor «sporbar tid». Tid fra GNSS eller NTP-servere[4] viser nøyaktig nok tid for de fleste formål, men ivaretar ikke sporbarheten til tids-angivelsen.

2.2.1 Tidssignaler fra satellitter

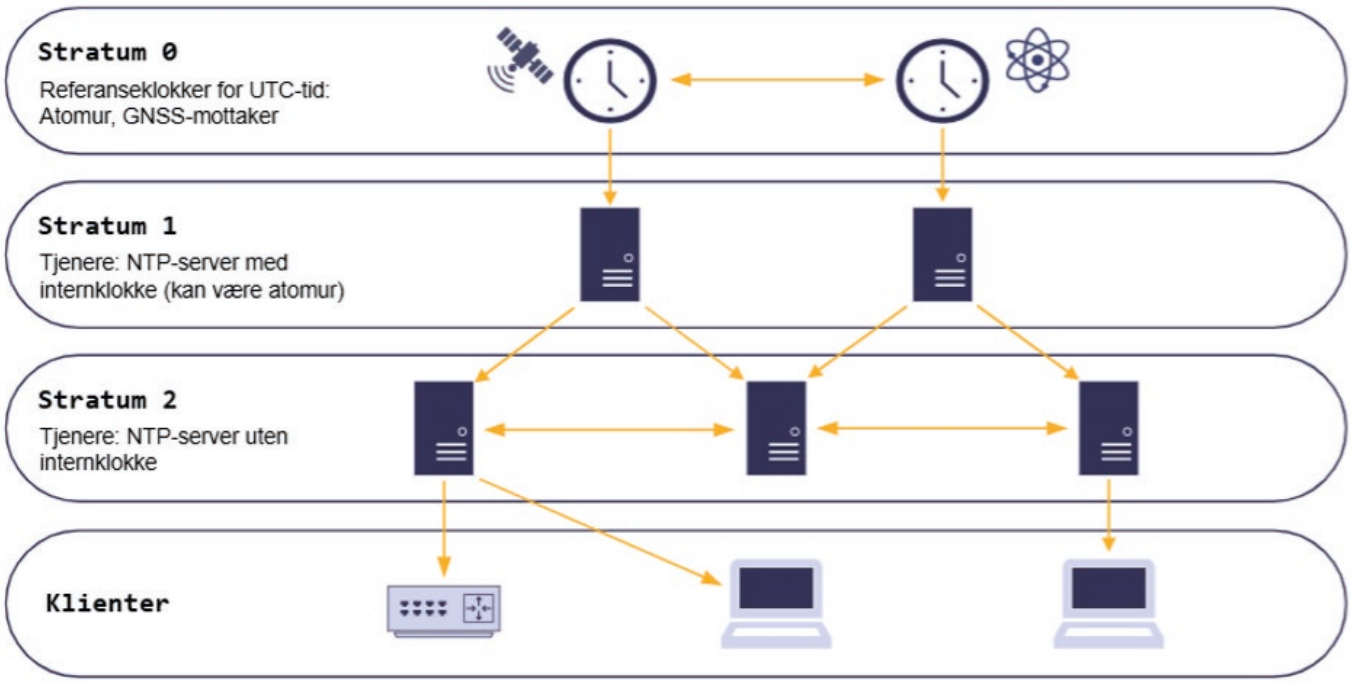
Ulike sektorer og virksomheter har hver sine løsninger for å hente nøyaktig tid. Veien fra den opprinnelige tidskilden og fram til brukeren, kan være lang og uoversiktlig.

I dag er det vanligste å bruke signaler fra GNSS for å få en felles tidsreferanse i samfunnet. Man trenger kun en antenne og en mottaker for satellittsignaler, noe som har vært billig og lett tilgjengelig siden GPS åpnet for allmenn bruk i 1993. Problemet er at man samtidig introduserer muligheter for å forstyrre GNSS-signaler gjennom for eksempel spoofing.

2.2.2 Tidsfrekvenser fra atomklokke

En atomklokke teller svingninger til et atom (f.eks. rubidium eller cesium). En høy og stabil frekvens på svingningene gir svært nøyaktig tid i en lengre periode, før den må korrigeres. Korrigeringen skjer gjennom å hente en frekvensreferanse fra en annen tidskilde, enten direkte fra en GNSS-mottaker eller indirekte gjennom optisk fiber fra en annen tidskilde.[5]

Figur 2. NTP er lagt opp med en hierarkisk klient/server-arkitektur hvor en klient (brukerenhet) synkroniserer sin klokke mot en eller flere servere.



Kilde: nsm.no/getfile.php/133693-1592905886/NSM/Filer/Dokumenter/U-09_Sikring_av_NTP.pdf, s. 6.

4 Network Time Protocol, et nettverk av servere for tidssynkronisering.

5 For eksperter er det ikke helt presist å bruke begrepet «atomklokke». Det korrekte er en «atomær frekvensreferanse» eller «atomær oscillator». Oscillatoren har ingen formening om klokkeslett – den har kun en jevn takt. Oscillatoren trenger en klokkegenerator for å lage signaler til en klokke, som viser tid.

2.2.3 Distribusjon av tid

Network Time Protocol (NTP) brukes til å synkronisere tid mellom datamaskiner og servere via internett. NTP-tidsservere sørger for at alle enheter i et nettverk har konsistent tid med millisekund-nøyaktighet. Serverne i stratum 1 (se figur 2) får frekvens fra svært nøyaktige kilder som atomklokker eller GNSS. Jo lenger unna man er den opprinnelige tidskilden (stratum 0), desto mindre sporbar blir tiden.

Enhetene i nettverket spør NTP-serveren om riktig tid og justerer sin lokale klokke basert på denne. I Norge leverer Justervesenet offentlige NTP-tjenester til bruk for egen tidssynkronisering. I systemer som krever nøyaktighet på mikrosekundnivå, brukes Precision Time Protocol (PTP-server) sammen med optiske fiberkabler.

Private og offentlige virksomheter henter sin tid fra ulike kilder (typisk NTP-servere, internett eller sky-tjenester som Microsoft Azure) og kjenner ikke nød-vendigvis til den opprinnelige tidskilden. Dette gjør det vanskelig å spore årsaken til ev. tidsfeil. At stadig flere overfører datasystemer til skytjenester, reduserer kontrollen på hvor tiden kommer fra.

2.3 Hvordan satellittbasert tid kan manipuleres

Radiosignaler for PNT sendes fra navigasjons-satellitter, som går i bane ca. 22 000 kilometer over jorda[6]. Signalene er veldig svake på bakkenivå og kan påvirkes av refleksjoner eller andre radiosignaler. En angriper kan bruke en programmerbar radiosender (SDR)[7] til å etterlikne satellittsignaler. Ved hjelp av en antenne rettet mot målet, kan angriperen sende manipulerte signaler som er litt sterkere enn de ekte.

6 Også kalt mellombane. Satellittkonstellasjoner er plassert i baner med hensikt om en bestemt fart, avstand og dekningsområde.

7 Software Defined Radio

Foto: Colourbox

Mottakerenheten låser seg på de sterkeste signalene og begynner å angi feil tid. SDRen fjernstyres ved hjelp av en datamaskin eller mikrokontroller.

Avstanden man kan ha mellom «spooferen» (radiosenderen) og målet er avhengig av hvor kraftig senderen er. Rekkevidden for spoofing kan være fra noen titalls meter til flere kilometer. Det er lite åpen informasjon om presis rekkevidde for spoofing, siden det er en ulovlig aktivitet.

Det er mulig å kjøpe SDR-radioer med programvare laget på ekte GNSS-signaler. Spoofing krever likevel at de falske signalene synkroniseres med de ekte satellittsignalene lokalt, slik at mottakeren gradvis begynner å følge de falske signalene uten å oppdage avvik. Hvis spoofingen starter for brått eller sender for sterke signaler, vil mottakeren ofte oppdage uregelmessigheter og avvise signalene. Spooferen må sende sterkere signaler enn de ekte, men ikke så sterke at de lager forstyrrelser og vekker mistanke. Spoofing krever avansert programvare og presis kontroll. Tiden det tar å innstille spooferen kan være fra minutter til mange timer, avhengig av utstyr.

Spoofing kan skje fra droner eller kjøretøy, men er enklere å håndtere fra en stasjonær radiosender pga. vekt og volum av radiosender, strømtilførsel og nøyaktig innstilling av antenne. Stasjonær plassering av en radiosender for eksempel på taket av en nabobygning med fri sikt til målets GNSS-antenne, kan være vanskeligere å oppdage og gi bedre mulighet for å presis innstilling av SDR-antennen.

2.4 NSMs risikovurdering

Nasjonal sikkerhetsmyndighet (NSM) trekker i rapporten Risiko 2025 spesielt fram risikoen for sabotasje og utfordringer knyttet til teknologiutvikling.

«Samfunnets avhengighet til satellittbaserte tjenester er en strategisk sårbarhet for Norge. Mange virksomheter baserer seg på tredjepartsløsninger som er avhengig av posisjon, navigasjon og tidsbestemmelse (PNT) og kommunikasjon fra satellitt. Eksempler på dette er sammenkoblede digitale systemer, meteorologi, navigasjon, logistikk og finansielle transaksjoner. Disse virksomhetene er i liten grad kjent med egen avhengighet til satellittbaserte tjenester gjennom tredjeparter.

Omfattende bortfall eller manipulering av PNT eller andre sentrale satellittbaserte tjenester vil ha store konsekvenser for samfunnet og totalforsvarets evne til å understøtte Forsvaret. Bortfall av presis tid fører for eksempel til problemer for samhandling mellom digitale systemer. Dette vil få store konsekvenser for samfunnet, virksomheter og individer, avhengig av hvilke systemer som rammes.» (NSM, Risiko 2025, s. 20)

2.5 Avhengighet av satellitter

Teknologirådet skriver i sin rapport *Teknologitrender for Stortinget 2026*, at antallet aktive satellitter i bane rundt jorda har økt fra 4 000 for fem år siden til nærmere 14 000 i dag. Kina har angivelig en ambisjon om å skyte opp 200 000 satellitter etter 2030. Satellitt-teknologi er blitt kritisk for moderne samfunn – fra kommunikasjon og navigasjon til militære operasjoner, jordobservasjon og finansielle transaksjoner. Både stater og selskaper konkurrerer nå om tilgang og kontroll i rommet.[8]

2.6 Hvem har ansvaret for «nøyaktig tid»?

En pålitelig og tilgjengelig kilde til nøyaktig tid er en felles innsatsfaktor som kommer hele samfunnet til gode. Ansvar og roller knyttet til nasjonale tids-

8 Teknologitrender for Stortinget 2026

tjenester er imidlertid ikke entydig plassert i en sektor eller ett departement. Justervesenet, som er underlagt Nærings- og fiskeridepartementet (NFD), har sentrale oppgaver gjennom sitt laboratorium med atomklokker og ansvar for Norges offisielle tid.

Nasjonal kommunikasjonsmyndighet (Nkom) har også en rolle med sitt ansvar for sikkerhet i digital infrastruktur og tilsyn med elektroniske kommunikasjonsnett, herunder tildeling av frekvenser for satellittkommunikasjon. Nkom er underlagt Digitaliserings- og forvaltningsdepartementet (DFD).

Samtidig finnes viktige brukere av tidstjenester i samtlige sektorer, og det operative ansvaret knyttet til driften av systemer som er avhengig av presis tid, ligger hos brukerne. Det innebærer at ansvaret for en pålitelig og tilgjengelig nasjonal tidstjeneste er sektorovergripende og ikke entydig plassert hos én aktør.

I motsetning til f.eks. Sverige og England, har ikke Norge en egen nasjonal tidstjeneste. En nasjonal tidstjeneste innebærer en infrastruktur med flere uavhengige atomklokker i et landsdekkende fibernett som brukere kan koble seg på. En slik tidstjeneste ble utredet av Justervesenet og NKOM i 2025[9] og fulgt opp med et oppdrag om å gjennomføre et pilotprosjekt i 2026.

9 Rapport: Kartlegging av behov og utredning av løsninger for etablering av en robust infrastruktur for distribusjon av presist og sporbart klokkesignal. Rapporten var åpen for innspill til 30. januar 2026.

3 Scenario

Utvalg og avgrensning av analyseobjekt
Samfunnet har de siste 30 årene blitt stadig mer avhengig av tjenester fra GNSS-satellitter. Faller de bort, blir samfunnet satt mange tiår tilbake[10]. De analoge og bakkebaserte systemene er bygget ned etter hvert som satellittene har gitt bedre og billigere løsninger. I vår analyse har vi valgt å konsentrere oss bare om tidssignaler, fordi langt flere virksomheter av avhengige av tid enn posisjon og navigasjon. Tid inngår dessuten i bestemmelse av posisjon og av navigasjon.

Hendelsesforløpet i scenarioet
I løpet av kort tid dukker det opp radiosendere og antenner montert på bygninger og master ulike steder i landet. Antenne synes knapt blant andre antenner. Det er radiosendere med avansert programvare (SDR) som settes opp. De sender falske signaler som ligner på GNSS-signaler, men er sterkere og overstyrer de ekte satellittsignalene. Hensikten er å «stille klokkene» i mottakerne av GNSS-signaler noen millisekunder fram.

Antennene på senderne rettes mot mål i nærheten, som er identifiserte gjennom etterretning. Målene er GNSS-mottakere på transformatorstasjoner som knytter sammen transmisjonsnettet og regionale strømnett, basestasjoner for mobiloperatørene, fly og flyplasser, banker, samt installasjoner langs veiene og i tunneler som brukes i trafikkstyringen. Også datasentre med konsentrasjoner av servere til private og offentlige virksomheter, er attraktive mål.

Etter noen dager registrerer Statnett spenningsfeil i deler av strømnettet uten å finne noen naturlig årsak. Flere regionale nett koples fra transmisjonsnettet for å opprettholde balansen på 50Hz. De berørte regionale nettselskapene skaffer alternativ tilførsel av kraft til nettet. Det dekker imidlertid langt fra strømbehovet i regionen og både næringsliv og husholdninger blir strømløse i flere dager.

En uke senere registrerer mobiloperatører at 5G-nettet i et større, tettbebygd område blir ustabilt. En basestasjon med en GNSS-mottaker mottar feil tid, og begynner å forstyrre datatrafikken til alle andre basestasjoner i samme dekningsområde. Kapasiteten i 5G-nettet faller, samtaler blir brutt og internett blir tregt og utilgjengelig. Mange mobile enheter kobler seg automatisk over til 4G-nettet, som ikke kan håndtere den samlede datatrafikken.

En stor bank blir nektet elektronisk tilgang både til børsen for å handle aksjer og valuta, og til Norges banks oppgjørssystem. Tiden banken opererte med var ikke i samsvar med Norges Banks og børsens tid; det var et avvik på flere mikrosekunder. Det blir slått alarm og alle transaksjoner blir satt på vent.

Det oppstår store forsinkelser i flytrafikken. Flyvninger kanselleres og fly i luften omdirigeres til andre flyplasser. Luftrommet stenges, og kontrolltårnene konsentrerer seg om å få ned flyene som er i luften på en sikker måte. Togtrafikken går omtrent som normalt.

10 «En dag uten satellitter», foredrag av Pål Brekke ved Direktoratet for romvirksomhet.

I veitrafikken oppstår det problemer både i noen store byer og på E18 og E6. Flere tunneler gir feilmeldinger og vegtrafikksentralene må stenge disse da de ikke har kontakt med nødtelefoner, bommer og vifter. Anleggsarbeid langs veiene stopper opp på grunn av manglende kommunikasjon og koordinering.

En rekke offentlige og private virksomheter mister tilgang til kritiske IT-systemer. Etter dager med feil-søking rettes mistanken mot spoofing av GNSS-mottakere som de rammede virksomhetene har på to store datasentre.

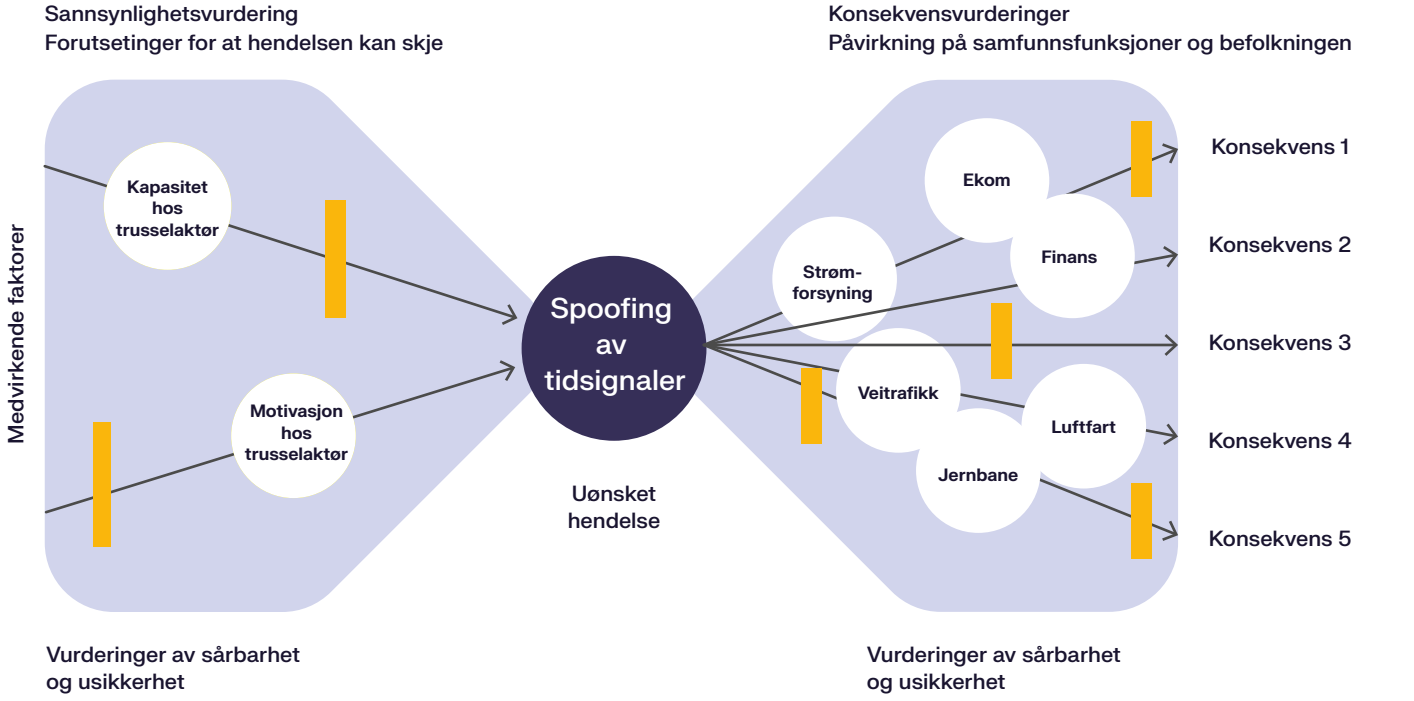
Nye problemer oppstår nesten daglig i en måneds tid. Nkom og politiet mistenker at det dreier seg om spoofing av GNSS-signaler, men det tar to uker før de sporer opp og fjerner de første senderne. Spoofingen fortsetter imidlertid mot stadig nye mål. Radiosenderne slås bare sporadisk på i fem minutter om gangen. I periodene hvor sendere er inaktive, kan de ikke oppdages. Det er ukjent hvor mange SDR-sendere som er plassert ut, hvilke mål de er rettet mot og hva som vil slutte å fungere i morgen. Hvem som står bak spoofingen, blir heller ikke avdekket.

4 Metode for risikovurderinger

Risikovurderingene i Analyser av krisescenarioer (AKS) bygger på en forståelse av risiko som usikkerhet om en hendelse vil inntreffe (angitt som sannsynlighet) og hva slags konsekvenser den vil få. Framgangsmåten følger trinnene i NS 5814: 2021 Krav til risikovurderinger, og omfatter vurderinger av sannsynlighet, samfunns-konsekvenser, sårbarhet og usikkerhet, som illustrert i figuren under.

Sårbarhet er en integrert del av risiko, siden systemets sårbarhet påvirker både sannsynligheten for at hendelsen kan inntreffe og konsekvensene den kan få. Et robust system har evne til å motstå og tåle en uønsket hendelse, mens et sårbart system mangler denne evnen i større eller mindre grad.

Figur 3. Sløyfemodell som illustrerer forløpet av hendelsen fra medvirkende faktorer via utløsende hendelser, til uønsket hendelse, og deretter følgehendelser og konsekvenser for samfunnet. Vurderinger av systemets sårbarhet og usikkerhet knyttet til kunnskapsgrunnlaget, gjøres som en del av sannsynlighets- og konsekvens-vurderingene. Stolpene i figuren illustrerer risikoreduserende barrierer i hendelsesforløpet.



5 Vurdering av sannsynlighet

Sannsynlighet er et uttrykk for hvor trolig vi mener det er at scenarioet vil inntreffe, gitt vårt kunnskapsgrunnlag. I AKS vurderer vi sannsynlighet ved å besvare to spørsmål:

1. Hvilke forutsetninger må være til stede for at hendelsen skal kunne inntreffe?

2. I hvilken grad er forutsetningene til stede i vårt analyseobjekt (det norske samfunnet)?

Forståelse av hendelsen og systemet som utsettes for hendelsen, er grunnlaget for vurderingen. Statistikk er til liten hjelp, da det er sjeldne og unike hendelser som vurderes i AKS.

Forutsetninger for omfattende spoofing av kritiske samfunnsfunksjoner er at:

- Kritiske samfunnsfunksjoner i stor grad bruker GNSS som kilde til nøyaktig tid, og særlig GPS
- Det er statlige aktører bak spoofingen med motiv om å skade, true eller presse Norge
- Aktørene har kapasitet bl.a. til å gjennomføre etterretning i forkant for å kartlegge sårbare punkter som kan spoofes
- Gjennomføring av spoofing krever spesialkompetanse
- Aktørene bak spoofingen bruker mellommenn til de tekniske installasjonene
- Spoofingen kan foregå i det skjulte lenge nok til å gjøre stor skade uten å bli avdekket

Vurderingen er at de to første forutsetningene i stor grad er til stede og utgjør sårbarheter, selv om enkelte samfunnsfunksjoner har moderne beskyttelse og redundans i form av flere tidskilder. Det er ikke kjent at noen aktører har motiv for å utrette så stor skade i Norge i dag. Samtidig kan vi anta at jo viktigere posisjon Norge får i NATO og europeisk forsvar, jo mer utsatt blir vi for fiendtlige handlinger og press. I en tilspisset situasjon kan lammelse av kritiske samfunnsfunksjoner svekke både militær og sivil motstandsdyktighet.

Etterretning ved bruk av åpne kilder kan avdekke mange funksjoner som er kritisk avhengige av satellittbaserte tidssignaler. Dette er felles sårbarheter for mange land.

Spoofing er relativt enkelt å gjennomføre hvis man har riktig kompetanse og en SDR-radiosender med kraftig antenne – utstyr som er fullt mulig å få kjøpt ulovlig. Organiserte aktører kan derfor ha kapasitet til å gjennomføre spoofing-aktivitet. Spoofing fra en fast lokasjon kan være lite synlig og vanskelig å detektere. Angrepet kan mistolkes som et cyberangrep og responsen derfor bli irrelevant. En spoofer kan slås av og på og dermed være usporbar i perioder.

Bruk av kunstig intelligens (KI) kan bidra til å øke omfanget av spoofing fordi KI kan trenes på ekte GNSS-data til å lage falske signaler med høy presisjon. KI kan dermed brukes til å simulere realistiske GNSS-signaler som matcher forventede mønstre, og dermed gjøre spoofingen vanskeligere å oppdage. Dessuten kan KI overvåke responsen fra målet og justere spoofing-signalet dynamisk for å unngå deteksjon eller for å manipulere tiden gradvis.

Man kan imidlertid beskytte seg mot GNSS-spoofing gjennom bruk av flere kilder til tid, f.eks. flere uavhengige atomklokker. Det er også mulig å ha mottakere som tar imot signaler fra flere GNSS-systemer (f. eks. GPS + Galileo + GLONASS), og

programvare for deteksjon og avvisning av unormale signaler. KI brukes også til å oppdage spoofing, ved å analysere signalmønstre og sammenligne med forventet oppførsel. Per i dag bruker likevel de aller fleste virksomheter, inkludert kritiske samfunns-funksjoner, enkle GPS-mottakere som sin primære tidskilde.

Spoofing mot norske virksomheter er praktisk og teknisk mulig. Målrettet spoofing mot kritiske samfunnsfunksjoner krever imidlertid et omfattende forarbeid (etterretning) og sterk motivasjon til å svekke norsk totalforsvarsevne. En vesentlig usikkerhet knyttet til om spoofingen blir vellykket, er hvordan GNSS-mottakeren motstår et angrep (avviser falske signaler), i hvilken grad falske tidssignaler sprer seg mellom datasystemene internt i nettverket og om systemene normaliserer seg etter angrepet (gjenoppretter riktig tid).

6 Påvirkning på kritiske samfunnsfunksjoner

Selv om spoofing kan påvirke folk direkte f.eks. gjennom at mobiltelefonen viser feil tid (og posisjon), er det først og fremst påvirkning av kritiske samfunnsfunksjoner som får alvorlige konsekvenser for samfunnet og befolkningen. Derfor har vi sett nærmere på hvordan samfunnsfunksjoner som har en kjent høy avhengighet av nøyaktig tid, kan bli rammet av spoofing.

Alle virksomheter er i praksis avhengige av nøyaktig og synkronisert tid for å fungere, siden de i stor og økende grad er digitaliserte. Enkle operasjoner som å logge på PC-en og å sende eposter, avhenger av flere systemer som samarbeider på basis av en felles tid. Tidssynkronisering er det som muliggjør informasjonsflyt innad i og mellom systemer, og binder det digitaliserte samfunnet sammen.

Resultatene av spoofing er usikre pga. manglende kunnskap og erfaring. Tester viser at ulike mottakere av GNSS-signaler håndterer manipulering av tid ulikt. Mens noen mottakere raskt detekterer og avviser falske satellittsignaler, lar andre seg enkelt lure (er

Tabell 1: Alle de kritiske samfunnsfunksjonene som var avhengige av PNT-tjenester, var avhengige av tid. Strømforsyning og ekom var bare avhengig av satellittenes tidssignaler.

Samfunnsfunksjon	P	N	T	Merknad
Opprettholde trygghet for liv og helse	x	x	x	Nødnett, SAR, SBAS/GBAS, ECDIS, satellittkommunikasjon
Opprettholde lov og orden	x	x	x	Politiet
Opprettholde finansiell stabilitet			x	Tidsstempling av transaksjoner
Opprettholde befolkningens behov for varme			x	Nøyaktig tid er sentralt for styring av kraftnett
Ivareta styring og kriseledelse	x	x	x	PNT sammen med jordobservasjon og satellittkommunikasjon
Ivareta nasjonal sikkerhet	x	x	x	Militære operasjoner, suverenitetshevdelse, havovervåkning
Beskyttelse av natur og miljø	x	x	x	Riktig navigasjon for å unngå havari, oljesøl
Vare. og persontransport	x	x	x	Luftfart, sjøfart, veitransport, jernbane
Elforsyning			x	Styring av kraftnett
Meteorologiske tjenester	x	x	x	Avhengig av jordobservasjoner og navigasjonssatelitter
Olje og gass	x	x	x	Dynamisk posisjonering
Elektronisk kommunikasjon			x	Tidssynkronisering

Kilde: På rett sted til rett tid - Nasjonal strategi for posisjonsbestemmelse, navigasjon og tidsbestemmelse (Samferdselsdepartementet 2018).

«naive»). Noen mottakere klarer heller ikke å gjenopprette riktig tid når spoofingen opphører[11]

Samferdselsdepartementet gjorde i 2018 en kartlegging av kritiske samfunnsfunksjoners avhengighet av satellittbaserte PNT-tjenester. Den viste at flere sektorer er avhengige av signaler for tid enn for posisjon og navigasjon.

Utvalget av seks sektorer som DSB har valgt å se nærmere på i denne analysen, baserer seg på denne kartleggingen og annen kjent kunnskap om sektorenes avhengighet av satellittbasert tid.

Hvor store avvik i tid som tolereres før systemene slutter å fungere, varierer avhengig av bruksområde, slik figuren under viser.

Figur 5. Ulike systemer har ulik toleranse for avvik i tid, fra år og dager til mikro- og nanosekunder. Kilde: NSMs Risiko 2025

Krav til nøyaktighet	Eksempel på bruksområder	Hva kan gå galt om tiden blir feil?
↑ år	Programvarelisenser	Programmer slutter å virke
	Sikkerhetssertifikater	Pålogging blokkeres
dag		
time	Tillitstjenester (pålogging, signaturer)	
minutt	Å rekke avtaler	
s	Industrielle kontrollsystemer	Styringskommandoer blir forkastet
	Banktransaksjoner	Transaksjoner går ikke gjennom
	Hendelseslogger	Virkning/årsak byttes om
	Aksjehandel	
300 km ms	Databaseoppdateringer	Gamle data overskriver nye
	Synkronisering av SG-basestasjoner	Redusert funksjonalitet eller stopp
30 m µs	Tidsstempling av målinger i kraftnettet	Feil i systemoversikt -> redusert kapasitet
	Luftromsovervåking	Redusert kapasitet
30 cm ns	Satellittnavigasjon	Redusert nøyaktighet, bortfall av tjeneste

Eksempler på bruksområder/tjenester som er avhengige av en felles tidsangivelse og hva som kan skje om krav til nøyaktighet blir brutt. Satellittnavigasjon stiller størst krav: Klokkefeil på et millisekund (1/1000 s) vil gi 300 km feil i posisjon på bakken. Forventet nøyaktighet på noen få meter krever klokker er synkronisert innenfor noen få nanosekunder (milliarddels sekund). Kilde: NSMs Risiko 2025.

11 Erfaringer fra jammertestene på Andøya

Under følger en utdypende gjennomgang av hver sektor.

6.1 Strømforsyning

Avhengighet av nøyaktig tid

Pålitelig strømforsyning er avhengig av balanse i strømnettet, dvs. at det produseres og forbrukes like mye kraft til enhver tid. Kraft er ferskvare og kan ikke lagres i nettet. I praksis er det kraftproduksjonen som må justeres etter forbruket i sanntid. For stor eller liten innmating av kraft i strømnettet i forhold til forbruket, kan føre til overspenning eller underspenning med påfølgende skader på utstyr og strømbrudd.

Strømforsyningen er avhengig av nøyaktig tid fordi hele kraftsystemet må være synkronisert for å fungere stabilt. Statnett overvåker og kontrollerer kontinuerlig balansen i det landsdekkende transmisjonsnettet og kan om nødvendig kople ut regionale nett med alvorlige feil, for å bevare balansen i transmisjonsnettet.

Det norske (og europeiske) strømnettet opererer med en frekvens på 50 Hertz (Hz) for å opprettholde balansen. Denne frekvensen er direkte knyttet til generatorer i kraftverkene, som kan justere produksjonen i sanntid. Kontrollsystemer bruker nøyaktig tid til å planlegge og utføre lastfordeling, slik at nettet holder seg i balanse. Den pågående digitaliseringen av strømforsyningen fører til stadig større avhengighet av nøyaktig tid.

Kilder til tid

Til nå har Statnett basert seg på GNSS-signaler som primærkilde til nøyaktig tid. Framover planlegges det for økt bruk av atomklokker som sekundær tidskilde og redundans mot feil tid fra GNSS. Den automatiserte overvåkingen og styringen av strømnettet forutsetter tidssynkronisering med nøyaktighet ned til mikro-sekunder.

Foto: Annika Byrde / NTB.

Spesielt kritiske funksjoner
Styringssystemene til Statnett får kontinuerlig sanntidsinformasjon fra avanserte sensorer (PMU[12]) som måler spenning, frekvens, last osv. i transmisjonsnettet. Dette gir en dynamisk overvåkning av kraftsystemet og feildeteksjon. PMU gir tidsstemplet data med høy presisjon ved hjelp av GPS. PMU måler mange punkter i nettet, og må være synkronisert i tid. Typisk foretas det 30–60 målinger per sekund i hvert punkt. Hvis det registreres avvik på mer enn +/- 0,1 Hz fra balansen på 50 Hz, må inntaket av kraft justeres.[13]

PMU-er plasseres typisk ved viktige knutepunkter i transmisjonsnettet, som store transformatorstasjoner, koblingsanlegg for flere linjer, nær store kraftverk og ved grensepunkter mellom regioner eller land. Det siste er kritisk for internasjonale kraftsystemer som Norden og Europa.

På de regionale nettene er det også enheter som samler inn data om status i strømnettet – RTU (Remote Terminal Unit). Disse er imidlertid enklere enn PMU. En RTU er en fjernstyrt enhet som samler inn data fra elektriske anlegg og sender det til nettselskapenes overvåkings- og kontrollsystem (SCADA-system). RTU fungerer som et bindeledd mellom feltutstyr (brytere, transformatorer, måleinstrumenter) og kontrollsenteret. Enheten kan utføre enkle kommandoer som å åpne/lukke brytere og overvåke alarmer og hendelser i tilnærmet sanntid.

RTU må være tidssynkronisert med styringssystemet, men har ikke behov for samme nøyaktighet som PMU på transmisjonsnettet. RTU plasseres typisk i regionalnettets transformatorstasjoner og koblingsanlegg, hos store forbrukere eller industrianlegg og i distribusjonsnettets endepunkter.

Manipulering av tidssignaler
Manipulering av tidssignaler i strømnettet kan foregå gjennom spoofing av GNSS-mottakere som sørger for at kontrollsentraler (styringssystem) og sensorer (PMU) får nøyaktig tid. Avvik i tid mellom sensorer og styringssystem skaper problemer for overvåking og styring av nettet i sanntid. Tidsfeilen kan se ut som en fasefeil og føre til utkobling av forbruk i et område. I det norske kraftnettet vil en slik fasefeil opptre ved et tidsavvik på 31,8 mikrosekunder eller mer.[14]

De regionale nettene får tiden fra GNSS. Den viktigste tidssynkroniseringen (millisekunder) er mellom kontrollsentralen og sensorene (RTU). Ved detektering av feil, har man imidlertid noen minutter på å reparere feilen før den får konsekvenser som kan medføre skade på utstyr eller strømbrudd. Tidsstempling fra RTU er viktig i de manuelle eller automatiserte analysene av feil.

Konsekvenser
Stor ubalanse i strømnettet kan føre til omfattende «blackouts», mens mindre avvik kan skade elektronikk. Manglende tidssynkronisering kan føre til at brytere og vern i nettet ikke reagerer tidsnok når det oppstår en feil. For å analysere hendelser og koordinere respons mellom ulike stasjoner på transmisjonsnettet, må også tidsstemplene være ekstremt presise.

Nettselskapet må iverksette egen regional kraftproduksjon («øydrift») hvis det mister kontakten med transmisjonsnettet, eller bruke linjer fra andre regionale nett. En slik beredskap vil ikke gi tilstrekkelig strøm til alle abonnenter i regionen.

Noen nettselskaper med eldre transformatorstasjoner har valgt å beholde en del konvensjonell teknologi som robusthet mot teknologiske feil. Det gir mulighet for noe

12 Phasor Measurement Units

13 energiteknikk.net/2020/02/statnett-vil-installere-500-sanntidsmalere

14 Det er vist i et amerikansk forskningsprosjekt at man på få minutter kan skape en større tidsfeil ved å spoofe kritiske enheter i kraftnettet (https://rnl.ae.utexas.edu/images/stories/files/papers/spoofSMUCIP2012.pdf)

manuell overvåking og feilretting. Nye transformator-stasjoner er mer digitale og automatiserte.

Sårbarheter
Styringssystemene i kraftsektoren bruker RTU- og PMU-sensorer for å overvåke nettet og alle enhetene i systemet må være nøyaktig synkronisert i tid. Enhetene bruker tidssignaler fra GPS-systemet og kan være sårbare for spoofing slik at de får feil tid.

6.2 Digital infrastruktur

Elektronisk kommunikasjon er avhengig av nøyaktig tidssynkronisering for å tilby effektiv telefoni og internett. Når man bruker 5G mobilnett, laster mobilen ned informasjon på samme frekvens som det laster opp informasjon. Fordi man kun opptar én og ikke to frekvenser for opp- og nedlasting, kan nettet håndtere mer trafikk samtidig. Dette medfører et spesielt strengt krav til tidssynkronisering: basestasjoner må være synkronisert innenfor ±1,5 mikrosekunder fra UTC, noe som innebærer et maksimalt gjensidig avvik på 3 mikrosekunder mellom basestasjoner.

Transportnettet er fiberbasert og utgjør ryggraden i det norske ekom-nettet, og ruter og transporterer datatrafikk mellom byer, regioner og ut mot internasjonale knutepunkter. Telenor sitt transportnett utgjør sammen med om lag 9000 tilknyttede base-stasjoner det største nettet i Norge. Basestasjonene fungerer som knutepunkter mellom brukere av mobile enheter (mobiltelefoner) og resten av nettet. I 2026 har både GlobalConnect og Altibox egne landsdekkende transportnett i tillegg til Telenor.

Det finnes tre mobiloperatører som eier og drifter egne fysiske mobilnett med antenner, basestasjoner og infrastruktur: Telenor, Telia og Ice. I tillegg er det en lang rekke tilbydere av mobiltjenester som leier kapasitet i disse nettene.

Mobiltelefoner som iPhone, Samsung osv. bruker en kombinasjon av mobilnett og GNSS for å synkronisere eget klokkeslett. Tiden til operatøren til mobilnettet prioriteres som kilde i mobiltelefoner, men om mobil-dekningen blir svak så kan mobiltelefonen benytte tidssignaler fra GNSS.

Kilder til tid
Alle basestasjoner må ha lik tid for å fungere sammen. Telenors infrastruktur er inndelt i geografiske regioner med hver sine «grandmastere». Grandmastere henter nøyaktig tid fra satellitter[15] og distribuerer den til alle basestasjoner via fibernett. Telenor bruker et grand-master-par som begge har en GNSS-mottaker, og en har atomklokke.[16] Grandmasterne forkaster signaler med for stort tidsavvik. Hvis satellittsignalet blir forkastet eller utilgjengelig, holder atomklokkene fortsatt riktig tid i en lang periode. Om én grandmaster likevel får forstyrrelser, tar den andre over.

Nasjonal kommunikasjonsmyndighet (Nkom) regulerer frekvensbruken og stiller tekniske krav som forutsetter at operatørene følger en felles tidsreferanse (UTC) for å unngå interferens. I 5G-nettet innebærer dette at alle operatører må være synkronisert mot UTC for at sending og mottak skal skje i samme tidsvindu. Sendere og mottakere på basestasjoner kan få tid direkte fra GNSS, og er dermed mer sårbare for forstyrrelser i tidssignaler.

Konsekvenser
Dersom en basestasjon får feil tid, vil all trafikk mellom mobile enheter og basestasjoner over 5G-nettet i samme dekningsområde bli ustabilt. Når base-stasjonene til én operatør har en annen tid enn andre operatører, begynner deres basestasjoner å sende på

15 UTC-tid fra GPS og Galileo.
16 Ref. stratum-figur, som viser hvordan nettverk for tidssynkronisering er satt opp hierarkisk.

tidspunkter hvor andre basestasjoner mottar. Selv om operatørene har fått tildelt ulike frekvenser, vil ulik tid føre til at 5G-signalene forstyrrer hverandre.

Basestasjonene kan fortsette å levere 4G om 5G-nettet blir utilgjengelig, men med betydelig mindre kapasitet. Uavhengig av hvilken operatør man bruker, kan det være vanskelig å ringe og samtaler blir brutt, tekstmeldinger blir ikke sendt, og mobilt internett vil bli svært tregt eller falle helt ut.[17] Dette kan føre til at tjenester som for eksempel mobilbetaling og Helsenorge blir utilgjengelig. Innbyggere og virksomheter som benytter mobilt bredbånd hjemme eller på arbeidsplassen kan få dårligere internett-tilgang, mens de som bruker fibernett vil fortsatt ha tilgang til internett.

Sårbarhet

Operatører av mobilnett har ansvar for egen nøyaktig tid, og benytter ulike tidskilder. Det kan være lokale GNSS-mottakere på basestasjoner eller regionale grandmastere som distribuerer tid over fibernett. Samtidig kan alle operatører bli påvirket av tidsforstyrrelser hos én operatør, siden signalene forstyrrer hverandre.

I en situasjon hvor landet er truet, er det avgjørende med rask og pålitelig kommunikasjon, både for myndigheter og befolkningen. Spoofing av GNSS-

17 Dersom tidskilder for en hel region utsettes for vellykket spoofing, kan også 4G-nettet gradvis miste avanserte funksjoner som ellers gjør det i stand til å håndtere økt trafikk.

Foto: Gorm Kallestad / NTB

mottakere på basestasjoner kan derfor redusere motstandsevnen.

Datasentre

Ved utgangen av 2025 var det registrert 54 kommersielle aktører og totalt 88 datasentre i Norge.[18] I dag er det kundene som hver for seg sørger for tilgang til nøyaktig tid for sine servere i datasenteret. Det kan skje gjennom en NTP-tidstjeneste eller ved at de monterer en GPS-antenne på taket til datasenteret. Ulempen er at mange GPS-antenner på samme tak kan være et attraktivt mål å spoofe – ett angrep kan ramme mange virksomheter. Datasentrene opplever ingen etterspørsel etter en tidstjeneste i dag, men antar at dette kan endre seg etter hvert som stadig flere blir avhengige av nøyaktig tid.

Eidsiva Digital datasenter skiller seg ut fra andre datasentre ved at det eid av offentlige virksomheter og ligger i en fjellhall. Kundene er offentlige virksomheter eller virksomheter med særskilte sikkerhetsbehov. De ser behovet for å tilby en sikker tidstjeneste til sine kunder og vil gjerne ha utbygging av en nasjonalt kontrollert tidstjeneste med et nettverk av autonome regionale atomklokker.

6.3 Finansielle tjenester

Avhengighet av tid

Sikker tid er nødvendig i hele det finansielle systemet for at IT-systemene skal kunne kommunisere med hverandre og for å gjennomføre finansielle transaksjoner. «Sikker tid» innebærer svært nøyaktig, synkronisert og sporbar tid i det integrerte finanssystemet, som bl.a. omfatter handel på børsen, finansielle transaksjoner mellom bankene og Norges Banks oppgjørssystem.

Norges Bank er «bankenes bank». Et avgjørende element i det norske betalingssystemet er Norges Banks oppgjørssystem (NBO). NBO skal sikre effektive oppgjør av betalinger mellom banker og andre foretak som har konto i Norges Bank. Flere av bankens funksjoner er skjermingsverdige verdier underlagt sikkerhetsloven.

Alle elektroniske betalinger i norske kroner gjøres opp mellom bankene i NBO, for å sikre finansiell stabilitet. Det gjelder både vanlige betalinger for husholdninger og bedrifter, store betalinger i finans- og valutamarkedene og utbetalinger av lønninger til offentlige ansatte og trygd. Gjennomsnittlig daglig omsetning i NBO var 350 mrd. kroner i 2024. NBO håndterte 4 600 betalingsoppdrag daglig og hadde kontoer for ca. 100 banker.

Både dagens systemer og ikke minst framtidens oppgjørssystem med en nasjonal beredskapsløsning, som begge var under utredning i 2025, har behov for nøyaktig og synkronisert tid distribuert gjennom et system med høy grad av nasjonal kontroll.

Kilder til tid

Norges Bank benytter i dag tre teknologier for tidssynkronisering: GNSS (GPS og Galileo), den svenske nasjonale NTS[19]-tjenesten Netnod og NTP via eksterne leverandører (som skytjenester). Øvrige banker bruker ulike løsninger for å skaffe seg nøyaktig tid og ulike plattformer i bankene har også ulike tidskilder. Det finnes ingen felles tidsinfrastruktur for bankvesenet. Norges Bank mener at tilgang til en pålitelig felles nasjonal tidstjeneste ville ha bidratt til å øke redundansen for brukere av Norges Banks IT-systemer, og gjøre det finansielle systemet mer robust.

18 nkom.no/datasenter/oversikt

19 Network Time Security

Konsekvenser
Bankene som handler på børsen, må ha korrekt og synkronisert tid. En handel krever presise tidsstempler ned til mikrosekundnivå for å sikre sporbarhet og overvåking av handelen. Oppgjørssystemer som NBO og VPS[20] er avhengige av korrekte tidsdata for å matche transaksjoner, dvs. sørge for et felles tidsvindu for oppgjør mellom selger og kjøper.

Lovpålagt tidssynkronisering mellom børs, oppgjørssystem og tilknyttede aktører (som banker), ble innført gjennom EUs MiFID II- regelverk i den norske verdipapirloven i 2018. Før dette fantes det ikke krav om mikrosekund-presisjon. Teknologiske krav til tid kom først med digitalisering og algoritmehandel. Nå kreves presise tidsstempler synkronisert til UTC med høy nøyaktighet: Kravet til høyfrekvent handel i sanntid er et avvik i tid på maks. 100 mikrosekunder, mens kravet for ordinær handel er maks. avvik på 1 millisekund. Dette kan ikke løses ved å bruke NTP, som mangler sporbarhet av tidsangivelsen.

Direkte personrelaterte systemer er ikke så tidssensitive, slik som betalingsterminaler, VIPPS osv. Bankkort kan brukes selv med tidsforstyrrelser. Integriteten i dataene opprettholdes med en unik ID og ikke tidsstempelet. De fleste slike betalinger samles, avregnes og gjøres opp fem ganger hver bankdag. Transaksjoner som lønninger til offentlig ansatte og trygd kjøres ut som masseutbetalinger på bestemte datoer og er heller ikke tidskritiske.

Det internasjonale betalingssystemet SWIFT er heller ikke så sårbart. For å sikre integriteten har SWIFT sin egen tidsserver som sikrer at alle som kommuniserer med hverandre via dette systemet har det samme forholdet til tid i meldingsutvekslingen.

Usynkronisert tid i en bank fører til at en handel ikke går gjennom og kan få store konsekvenser. Finanstilsynet kan ilegge gebyr eller straff ved brudd på MiFID II-krav, inkludert manglende tidssynkronisering. Gebyrene kan være betydelige, og regelverket krever at foretak dokumenterer at tidssynkronisering er korrekt. I EU har slike brudd ført til bøter i millionklassen. I tillegg risikerer banken å tape store verdier og omdømme på tapt handel.

For bankene er den viktigste verdien evnen til å utføre handel i markedet. Derfor er ukorrekt tid svært kostbart og nøyaktig tid lønnsomt. Det kan foretas 100 handler i sekundet, og tidsstempling og logging er avgjørende for å dokumentere at det går riktig for seg. En del handel er overtatt av KI og fører til flere kjøp på kortere tid (mikrotransaksjoner). Antall handler i løpet av ett døgn er stigende fordi det er mer automatikk; meglere er delvis erstattet av roboter.

Norges største bank, DNB, benytter i likhet med mange andre europeiske storbanker et datasenter utenfor London til deler av sin handelsplattform, amerikansk eide Equinix. Det antas at Equinix har cesium frekvensgeneratorer som dytter en stabil frekvens uavhengig av GNSS-signaler.

Sårbarhet
Banker og andre aktører i finansmarkedet bruker ulike kilder til tid med ulik GNSS-avhengighet. At det GNSS-baserte tidssignalet forsvinner er ikke kritisk så lenge man har sekundære tidskilder. Men om klokkene innad i et system[21] har ulik tid, kan det gå veldig galt. Problemet er intern uenighet om hva tiden er og ikke bortfall av tid. Spoofing kan føre til usynkronisert tid internt i den enkelte bank og i banksystemet.

20 Verdipapirsentralen

21 Hele det sammenvevde finansielle systemet eller bankenes egne systemer.

6.4 Luftfart

Avhengighet av nøyaktig tid

De siste tiårene har tjenester for planlegging, overvåkning og styring av lufttrafikken blitt stadig mer digitalisert og dermed mer avhengig av nøyaktig tid. Dette innebærer blant annet en overgang fra lokale enheter til sentraliserte digitale systemer: Lokale tårn på flyplasser erstattes med sentre for digitale tårn, der lufttrafikktjenesten[22] kan styre flere flyplasser i landet samtidig[23]. Mer avanserte systemer for kommunikasjon, navigasjon og overvåkning på bakken og i lufta gjør flyplassene og flyvningene mer effektive, og muliggjør flere samtidige flyvninger.

En overordnet trend er at stadig flere lufthavner går over fra bakkebaserte til satellittbaserte innflyvningsmetoder. Bruken av radarer på bakken for å overvåke luftrommet erstattes i stor grad av sendere på flyet som rapporterer flyets GNSS-posisjon til bakken. Dette gjør at luftfarten er, og vil bli mer sårbar for GNSS-forstyrrelser.[24]

Den tradisjonelle kommunikasjonen mellom fly og lufttrafikktjenesten er tale via radio. Dette erstattes gradvis med kommunikasjon via satellitter, i form av digitale meldinger på skjermene som trenger tidsstempler[25].

Digital fjernstyring av tjenestene på lufthavner krever meget nøyaktig tid. På flyplassene er det installert sensorer med kameraer, mikrofoner og annet overvåkningsutstyr, som dekker rullebaner og luftrommet rundt. Video, lys og sensorer fungerer uavhengig av hverandre, og overfører det man ville kunne se og sanse i et lokalt tårn til et samlet, digitalt bilde i tårnsentralen.[26] Sensorene må fungere som et samlet system, og forutsetter derfor at de har samme tidsreferanse.

Fly har flere kritiske funksjoner som er avhengige av korrekt tid, blant annet for å verifisere kartdata, beregne flyets posisjon og bane, styre autopilot og varsle om mulig kollisjon med terreng og andre fly. Disse funksjonene styres av Flight Management System (FMS), en datamaskin som er hjernen i en moderne cockpit. FMS hjelper pilotene med å planlegge, styre og overvåke flyvningen fra start til landing.

Kilder til tid

Flere tidskilder benyttes i luftfarten, men i praksis er det GNSS som brukes mest[27]. Fjernstyring av lufthavner foregår gjennom stamnettet[28], som mottar tidsreferanser fra fire sentrale atomklokker. De fleste lufthavner har også lokale atomklokker. Ved bortfall av GNSS vil atomklokkene holde på tiden i en bestemt periode. Bagasjesystemer og informasjonstavler på de enkelte lufthavnene bruker det administrative nettet, som er avhengig av en felles tid, men ikke like nøyaktig som stamnettet.

Alle kommersielle fly er utstyrt med en GPS-mottaker, som brukes både til å sende posisjonsdata til sensorene på bakken og som også fungerer som tidskilde for flyets interne datamaskin. Kommunikasjon via digitale

22 Omfatter både kontroll og flygeinformasjon.

23 Remote Tower Centers i Bodø er i dag verdens største senter for fjernstyrte tårn, hvor det per i dag er cirka 11 lufthavner i operativ drift. Innen 2027 vil 21 lokale og regionale flyplasser være fjernstyrt.

24 www.nrk.no/nordland/ny-flyplass-i-rana-blir-berre-bygd-med-gps-og-gnss-og-utan-andre-innflygingssystem-1.17641173

25 Også kalt datalink, ved hjelp av egne satellittsystemer for kommunikasjon.

26 om.avinor.no/flysikring/digitale-tarn/

27 Hovedsakelig amerikanske GPS.

28 Også kalt nettverk for flyoperative data

meldinger er avhengig av at tiden i flyets interne datamaskin er lik den hos lufttrafikktjenesten[29].

En viktig funksjon i flyet å verifisere at FMS benytter gyldige data om blant annet ruter, prosedyrer og luftromsrestriksjoner. FMS krever en oppdatering hver 28. dag, når ny data kunngjøres internasjonalt. Når denne bestemte datoen er nådd, gir FMS beskjed at den eksisterende dataen er ugyldig.[30]

Konsekvenser

Avinor har så langt ikke erfart forstyrrelser av tidssignaler på bakken. Selv om stamnettet til tårnene kan ha korrekt tid, vil styring og overvåkning av luftfarten likevel bli forstyrret dersom fly blir spoofet. I kontrollrommet kan et fly i verste fall fremstå på to steder samtidig, og hele eller deler av luftrommet forsvinne fra overvåkingsbildet. Da må trafikken i luftrommet begrenses og flyplassen stenge. Det samme vil også gjelde for tårn som er bemannet lokalt.

Hvis et fly blir utsatt for GNSS-spoofing, påvirkes tiden til den interne datamaskinen og dermed alle tidsavhengige funksjoner i flyet. Små tidsavvik kan gjøre at digitale meldinger mellom fly og lufttrafikktjenesten stopper opp, og klareringer og informasjon må håndteres manuelt over radio.

29 En «datalink» via kommunikasjonssatellitter gjør det mulig å utveksle digitale meldinger mellom fly og flygeleder, men disse meldingene tidsstemples via flyets interne datamaskin, som hentes fra GPS.

30 I henhold til AIRAC-systemet, et internasjonalt system som sikrer at denne informasjonen kunngjøres og oppdateres på samme tid for alle fly.

Foto: Colourbox

Dersom systemtiden i flyet flyttes langt nok frem i tid, vil FMS forkaste det eksisterende kartgrunnlaget uten at et gyldig kartgrunnlag er tilgjengelig[31]. Dersom forskyvning i tid påvirker beregningen av posisjon, kan i tillegg autopilot og terrengvarslingssystemet slutte å fungere, noe som fjerner et viktig sikkerhetsnett i cockpit.

Nyere fly med mer sofistikerte systemer er vanskeligere å spoofe, men vellykket spoofing vil skape desto flere og mer komplekse problemer. På den andre siden vil eldre og mer analoge fly være lettere å spoofe, men gi mer begrensede og forutsigbare problemer.

Vellykket spoofing kan skape tekniske følgefeil i utstyret og instrumentene som er tilknyttet flyets datamaskin, slik at problemene vedvarer også etter at spoofingen har opphørt. Avinor sin erfaring er at få fly er i stand til å nullstille FMS og GNSS-mottakere i luften. For å rette feilene, må flyet derfor lande. Selv om flyene i luften fortsatt kan manøvreres, vil luftrafikktjenesten mangle full oversikt og kontroll[32]. Det medfører bruk av nødløsninger og manuelle prosedyrer. Planlagte flyvninger blir derfor kansellert og fly i luften må omdirigeres til andre flyplasser. Dette kan skape utfordringer ettersom mengden drivstoff i flyet er nøye planlagt ut ifra ruten, særlig om dårlig sikt kan begrense mulige lufthavner for landing. På lufthavner uten anlegg for bakkebasert innflyvning vil det ikke være mulig å lande uten GNSS.

Sårbarheter

EU har planer om å effektivisere luftrommet ytterligere, slik at alle flyvninger foregår i nøye kalkulerte og fastlagte baner. Avinor beskriver at dette kan være en effektivisering som gir økt sårbarhet, ettersom nøyaktig tid vil bli enda mer kritisk. En digitaliseringstrend i luftfarten, er økt bruk av GNSS fremfor bakkebaserte innflyvningssystemer. En del eldre utstyr på norske lufthavner bruker kun amerikanske GPS. Det er ingen overordnet koordinering i bruk og synkronisering av tidskilder internasjonalt.

En enkelt SDR-sender kan nå mottakere både på bakken og fly i luften. Ifølge Avinor er det sannsynliggjort at en relativt svak sender på 1 watt vil kunne forstyrre GNSS-mottakere i en radius opp til 50 kilometer[33]. Innenfor denne sonen vil Flight Management System (FMS) kunne avvise flyets kartgrunnlag, svekke digital kommunikasjon med tårnet og føre til at navigasjon og anti-kollisjonssystemer slutter å fungere. Overvåkning av luftrommet og bakken blir upålitelig, og skjermene i cockpit kan vise noe annet enn skjermene i tårnene.

På flere lokale og regionale flyplasser vil bakkebaserte innflyvningssystemer avvikles eller reduseres til fordel for satellittbaserte innflyvningsprosedyrer fram mot 2030[34]. Uten tilgjengelig GNSS eller kartgrunnlaget i FMS kan fly kun lande på flyplasser med bakkebaserte innflyvningssystemer hvis det er dårlig sikt. I et slikt scenario vil det dermed være færre tilgjengelige flyplasser for landing.[35]

Det er omkring 400 000 ruteflyvninger innenlands i året[36]. I tillegg til kommersielle flyvninger, vil de mer enn 30 000 årlige ambulanseflyvningene, særlig mellom sykehusene i Nord-Norge, være sårbare for GNSS-forstyrrelser.

31 Avhengig av hvor nærme flyets datamaskin er den 28. dagers syklusen på kartdata (AIRAC).

32 Kontrolltårnet benytter signaler fra flyene i overvåkningen av luftrommene

33 Det er usikkerhet knyttet til om forsøk på spoofing over slike avstander vil gi for sterk støy for å tolkes som et autentisk satellittsignal.

34 Dette er blant annet knyttet til høye kostnader for vedlikehold og utbytting av utstyret som brukes på bakken. PBN Transition Plan i Navigasjonsstrategi for luftfart i Norge beskriver også at innflyvning basert på GNSS skal bli den sentrale infrastrukturen for luftfart, og kun mellomstore og store flyplasser skal av beredskapshensyn beholde bakkebaserte innflyvningssystemer. Dette er en generell internasjonal trend, og følger bl.a. European Commission Implementing Regulation 1048/2018, som er gjort gjeldende i norsk rett.

35 Som for eksempel ILS, LOC, VOR/DME eller NDB.

36 Det er 23 millioner registrerte ankomster og avreiser for innenlands flyvninger i året.

6.5 Jernbane

Bane NOR er i gang med å modernisere jernbanen ved å innføre et nytt, digitalt signalsystem ERTMS (European Rail Traffic Manangement Systems). ERTMS er et felles europeisk signalsystem for styring og sikring av togtrafikk. Det erstatter tradisjonelle analoge lyssignaler langs sporet med digitale signaler direkte til togets datamaskin og lokførerens skjerm.

ERTMS ble innført på de første strekningene i Norge i 2024 og skal etter planen rulles ut til hele landet innen 2034. Neste generasjon ERTMS, som innføres gradvis, er heldigitalt.

ERTMS består av tre ulike delsystemer som fungerer sammen: ett i sporet, ett i togene og ett trafikkstyringssystem ETCS[37]. Baliser er elektroniske sendere i jernbanesporet, som sender informasjon om posisjon til togene. GSM-R[38] er et lukket mobilnettverkssystem, som benyttes til kommunikasjon mellom lokfører og kontrollsenter. GSM-R sørger blant annet for bevegelsesautorisasjoner (hvor langt og hvor fort toget kan kjøre) fra trafikkstyringssentralene til togene.

37 European Train Control System

38 Global System for Mobile Communications – Railway er en felles europeisk standard for mobilkommunikasjon på jernbanen. Dagens GSM-R er basert på 2G-teknologi og systemstøtten for 2G vil opphøre tidlig på 2030-tallet. Neste generasjon kommunikasjonssystem vil være basert på 5G. oppslagsverk. banenor.no/network-statement/vedlegg/kommunikasjon-for-ertms/

Avhengighet av nøyaktig tid
ERTMS er helt avhengig av nøyaktig tids-synkronisering for at kommunikasjon og system-logikk mellom tog, spor og kontrollsystemet (ETCS) skal fungere effektivt. Trafikkstyringssentralen distribuerer korrekt og synkronisert tid via NTP-servere til alle signalsystemer for togfremføring i ERTMS, og fungerer som referansepunkt for tid i hele jernbanenettet.

GSM-R transporterer meldinger (kjøretillatelser, posisjonsdata og statusmeldinger) som er tids-stemplet. Basestasjoner i GSM-R sørger for at tog og kontrollsenter kan utveksle tidsstemplede meldinger i sanntid og synkronisere radiolinken mellom basestasjoner og tog.

Kilder til tid
Bane NOR har satt opp regionale klokkenoder som sørger for tidssynkronisering til egne GSM-base-stasjoner. De samme klokkenodene leverer riktig tid til NTP-servere, som igjen distribuerer riktig tid til systemer som brukes i togfremføringen, inkludert trafikkstyringssentralene. Klokkenodene består av GNSS-mottakere og en atomklokke. Klokkenodene overvåkes kontinuerlig, og det er satt opp en brannmur som kan oppdage og reagere på forsøk på jamming eller spoofing av tidssignalene.

ERTMS i Norge bruker GPS-tid som primær tidskilde, og trafikkstyringssentralen mottar tidssignalene fra NTP-serverne. Atomklokker brukes som back up ved bortfall av GPS-tid. Togene er utstyrt med egne GNSS-mottakere (for både GPS og Galileo), som gir en nøyaktig tidsreferanse for synkronisering av utstyret om bord i togene.

Konsekvenser
Forstyrrelser av tidssignaler vil påvirke kommunika-sjon, meldingsrekkefølge og logging, som igjen kan føre til at det ikke blir gitt kjøretillatelser. Tog vil gå i sikkerhetsmodus, kjøre med redusert hastighet eller stanse helt opp.

Sårbarhet
I neste versjon av ERTMS rapporterer togene selv posisjon kontinuerlig, noe som krever posisjons-bestemmelse – herunder GNSS-posisjon – og kontinuerlig kommunikasjon med kontrollsenter.
I dagens ERTMS skjer togdeteksjon i sporet gjennom bruk av akseltellere og er ikke avhengig av tid fra GNSS. I neste versjon (flytende blokk) er det mulig å fjerne eller redusere bruk av akseltellere. Det betyr at avhengigheten av nøyaktig tid til posisjonsbestemmelse av togene og posisjonsrapportering blir en direkte del av trafikkstyringen.

Hvis tiden ikke er helt riktig (millisekund-presisjon), blir usikkerheten i togenes posisjon større. Da må systemet øke sikkerhetsmarginene og kapasiteten på banen reduseres.

Det nye systemet for posisjonsbestemmelse i ERTMS øker sårbarheten ved bruk av GNSS, fordi GNSS-signaler kan spoofes.

6.6 Veitransport

Avhengighet av nøyaktig tid
Sikker og effektiv trafikkavvikling er avhengig av at sentrale overvåkings- og styringssystemer på veg-trafikksentralene (VTS) kommuniserer med automati-sert utstyr langs veien. Dette utstyret kan være sensorer, trafikklys, veglys, skilt og kameraer, samt bommer, vifter og nødtelefoner i tunneler. Vei-utstyret sender også stadig mer informasjon rett inn i kjøretøyene om f.eks. fartsgrenser, kø og ulykker. Den digitale kommunikasjonen i sanntid er avhengig av at styringssystemene, veiutstyret og kjøretøyene har nøyaktig lik tid for å fungere.

Å flytte tiden noen uker fram kan også få store konsekvenser. Blant annet kan SSL-sertifikater[39] plutselig gå ut over sin gyldighetsperiode og slutte å virke, og da mister man påloggingsmuligheter til sentrale systemer.

Tidskilder

Tid fra GPS blir benyttet som primærkilde i NTP-nettverket til Statens Vegvesen, som vegtrafikk-sentralene er tilknyttet. Ved bortfall av GNSS, benyttes internettid som alternativ tidskilde. Elektronisk veiutstyr får i hovedsak tid via mobilnettet og det kan oppstå manglende synkronisering av tid mellom vegtrafikksentralene og veiutstyret.

NTP tar bare automatisk over når GNSS-signalene blir borte f.eks. ved jamming. Ved spoofing mottar man tidssignaler selv om de er falske, så GNSS-tid vil fortsatt bli brukt. Et mindre avvik mellom GPS- og internettid er ikke uvanlig, så det vil ikke vekke mistanke om spoofing. Tidsfeilen vil få tid til å forplante seg til flere systemer og skape nye feil. Det er anslått at følgeskader av manipulering av tid kan ta dager og uker å rette opp i.

Statens vegvesen sentralt er i ferd med å etablere seg i et nytt datasenter med egen GNSS-mottaker. Det vil gi to uavhengige måter å hente GNSS-tid på. Bare to kilder til tid vil imidlertid ikke gi et entydig svar om hvilken som er feil, hvis det oppstår avvik. Veisektoren har ingen krav til hvordan nøyaktig tid innhentes og synkroniseres internt i dag.

Framtidens veitrafikk

Intelligente transportsystemer (ITS) er samlebetegnelsen for teknologien som skal effektivisere, sikre og gjøre veitrafikken mer miljøvennlig framover. Den vil samtidig gjøre veitrafikken mer digitalisert og avhengig av nøyaktig, synkronisert tid. Samvirkende ITS er teknologi og applikasjoner som utnytter effektiv datautveksling mellom enheter, aktører og infrastruktur i transportsystemet. Datautvekslingen kan skje mellom to kjøretøy eller mellom infrastruktur og kjøretøy.

Appen «Vegvesen trafikk», som ble lansert i 2025, benytter denne teknologien. Den gir trafikanter sanntidsinformasjon om kjøreforhold og status for fjelloverganger, broer og tunneler. Vegvesenet utreder om dagens Autopass-system for betaling av bompenger skal erstattes av satellittbaserte betalingsløsninger med flere samvirkende systemer.[40]

ITS er avhengig av nøyaktig synkronisert tid til:

- Posisjonsbestemmelse, som er nødvendig for navigasjon, ruteoptimalisering og flåtestyring.
- Innsamling av sanntidsdata om trafikkflyt, køer og hendelser, for å varsle trafikanter.
- Synkronisering av systemer og logging av hendelser i veitrafikken.

Konsekvenser

Veiutstyr som mister tidssynkronisering, vil forbli uendret, dvs. en bom som var nede vil forbli nede, selv om den får signal om å gå opp. Det kan hindre viktig informasjon til trafikanter og vegtrafikksentralenes mulighet til å overvåke og styre objekter langs veien, f.eks. stenging av tunneler. Da skal i utgangspunktet tunnelene patruljeres av entreprenørene, for å holdes åpne. Hvis en hel VTS-region faller ut på grunn av tidsfeil, blir det for mange tunneler å patruljere og man må prioritere hvilke tunneler som må stenges.

Elektroniske anlegg langs veien vil reagere ulikt på tidsfeil, bl.a. fordi noe utstyr er opptil 30 år gammelt.

39 SSL, «Secure Sockets Layer», gir mulighet til kryptert kommunikasjon og benyttes ofte for sikker innlogging til systemer på datamaskinen, inkludert både fjernstyring og VPN.

40 vegvesen.no/fag/fokusomrader/forskning-innovasjon-og-utvikling/avsluttede-programmer-og-prosjekter/smartere-vegtrafikk-med-its/samvirkende-its

I nye autonome systemer kan signaler fra brann-detektorene føre til automatisk stenging av tunnelene. I noen tilfeller kan VTS stenge tunnelen uten digital kommunikasjon. Andre tunneler kan stenges på stedet av lokalt brannvesen eller entreprenører.

Ulike tekniske løsninger fører til usikkerhet om hvordan utstyr vil reagere uten kommunikasjon med styrings-systemet (VTS). Nødtelefoner i tunneler kan feile. Det vil antakelig ringe hos VTS-operatøren når noen tar av røret på en telefon, men usynkronisert tid mellom telefonen og VTS kan føre til at samtalen blir forkastet. Dette er ikke noe Statens vegvesen har øvd på eller har god oversikt over.

Sårbarheter

Trafikantene har tillit til at trafikkinformasjon de får fra myndighetene er korrekt, enten den kommer i form av dynamiske skilt eller på skjermen i bilen. Dette er i økende grad sanntidsinformasjon som registreres av kameraer eller sensorer i veibanen. Hvis denne infor-masjonen skulle være feil fordi sensorene opererer med feil tid, kan det medføre både trafikkfare og svekket tillit til trafikkinformasjon.

Automatisert utstyr langs veiene er koplet til uavhengige lokale servere med egne tidskilder. Hvis disse serverne får feil tid, mister de kontakt med vegtrafikksentralenes overvåknings- og styrings-systemer.

Elektronisk utstyr langs veiene og i tunneler som får tid fra mobilnettet, er sårbare for spoofing av base-stasjoner i mobilnettet. Uten mobildekning, er GPS ofte backup.

Økt effektivitet i veitrafikken kan skape nye sårbarheter. Statens vegvesen er i ferd med å standardisere og sentralisere trafikkovervåkingen og -styringen, slik at en vegtrafikksentral kan overta for en annen som faller ut. En slik sentralisering forutsetter at alle bruker en felles sentral tidsangivelse og ikke egen regional tid. En tidsfeil i et sentralt styringssystem vil imidlertid ramme en større del av veitrafikken enn mange de-sentraliserte systemer.

Tidsavhengigheten blir stadig mer kritisk etter hvert som kjøretøyene blir «selvkjørende» eller autonome. Da kan også små forsinkelser i kommunikasjonen mellom kjøretøy og infrastruktur få store konsekvenser.

7 Identifiserte sårbarheter

Gjennomgangen av seks kritiske samfunnsfunksjoner viser at det er ulik sårbarhet (og sannsynlighet) for å bli rammet av spoofing og få feil tid i sine data-systemer. Konsekvensene for virksomhetene som rammes er også ulike. Gjennomgangen identifiserer etter DSBs vurdering sju faktorer som påvirker hvor sårbare samfunnsfunksjonene er for spoofing.

7.1 Faktorer som påvirker sårbarheten for spoofing

1. Ulike tidskilder
   Flere tidskilder satt riktig opp, kan skape redundans (se pkt. 7 under). Men det kan også skape sårbarhet hvis tidskildene ikke synkroniseres og gir interne systemer ulik tid.

   Store virksomheter har ofte mange datasystemer som er innført hver for seg over lang tid.

   F.eks. brukes atomklokker eller GPS til operasjonelle driftssystemer (OT) og internett-tid til de administrative systemene (IT). Ett system som mottar feil tid pga. spoofing, kan slutte å kommunisere med de andre eller overføre feil tid til disse. Det er generelt manglende innsikt og dokumentasjon av hvordan mottak, distribusjon og synkronisering av tid foregår internt i store virksomheter. Lang vei fra opprinnelig tidskilde til bruker forsterker problemene.

2. Grad av digitalisering
   Digitalisering av funksjoner og tjenester skaper økt avhengighet av nøyaktig og synkronisert tid. Tidsfeil i de operasjonelle driftssystemene (OT) får som regel mer direkte og alvorlige konsekvenser enn feil i informasjonssystemene (IT).

3. Avhengighet av mikrotid
   Krav til effektivisering og hurtigere dataflyt krever oppdeling av tid i stadig mindre enheter (tids-vinduer). Mens man før kunne ha et millisekund på å utveksle data, må man nå utveksle samme mengde data på et mikrosekund.[41] Det stiller høye krav til leveransen av tid og gir veldig små feil-marginer (toleranse for avvikende tid).[42]

4. Distribuerte systemer med sårbare ytre ledd
   Mange samfunnsfunksjoner krever sentralisert overvåking og styring i kontrollsentraler av elektro-niske komponenter i store geografiske områder. Kommunikasjon mellom styringssystemet og slike ytre ledd krever at de er tidssynkroniserte. Tid kan hentes fra mobilnett eller GPS. Ved bruk av GPS er de ytre leddene sårbare for spoofing (f.eks. digitaliserte elementer i kjøretøy, fartøy, fly og sensorer).

5. Åpne systemer
   Åpne nett med mange brukere, som f.eks. internett, gir mindre grad av kontroll enn lukkede systemer. Datakommunikasjon direkte med kjøretøy i vei-trafikken skjer på åpent nett, mens GSM-R system i jernbanen er et lukket nett.

41 Fra en tusendels sekund til en milliondels sekund.

45 En parallell mange kan kjenne seg igjen i er beskjeden fra for eksempel BankID om at «sesjonen er utløpt» om man ikke bekrefter innlogging i løpet av kortere tid.

6. Avhengighet av GPS
   De globale GNSS-satellittsystemene tilhører i dag stormaktene USA, Kina, Russland og Europa (EU). Amerikanske GPS er det klart mest brukte i vesten. I en sikkerhetspolitisk spent situasjon, kan kontroll over et GNSS-system være et effektivt «våpen». GNSS-satellittene kan programmeres til å ikke sende - eller sende feilaktige tidssignaler - til bestemte områder på jorda. Dessuten er det utviklet anti-satellittvåpen (ASAT), som er designet for å deaktivere eller ødelegge satellitter i rommet for militære eller strategiske formål (elektronisk krigføring). Å være avhengig av kun ett satellittsystem kan derfor være sårbart.

7. Manglende redundans
   I virksomheter med spesielt høye krav til nøyaktig, sikker og pålitelig tid, er ikke GPS eller NTP gode nok tidskilder. De må få tid direkte fra atomklokker enten som primær eller sekundær tidskilde, som tar over hvis primærkilden faller ut. Flere tidskilder kan altså skape god redundans. Klokkene må settes riktig opp i et hierarki internt, slik at den sikreste tidskilden overstyrer de andre. Tidskilder på samme nivå (f.eks. GNSS-mottakere) må bestå av minst tre uavhengige enheter for å skape flertall for riktig tid hvis de to klokker viser avvikende tid

   «NTP-tid» kan være både pålitelig og upålitelig. En NTP-server med egen GPS-mottaker eller atomklokke, og som distribuerer tiden i ett internt nettverk, gir dokumenterbar og pålitelig tid. Standardløsningen for NTP er imidlertid en frivillig «pool» av servere som distribuerer udokumenterbar tid over internett, såkalt «internett-tid». Justervesenet tilbyr en pålitelig NTP-tjeneste for UTC-tid på «ntp.justervesenet.no» (på millisekundnivå).

Tabellen under viser vår vurdering av hvordan de ulike faktorene påvirker sårbarheten for spoofing i de undersøkte sektorene.

Tabellen danner grunnlag for oppsummeringsfigur 6 i kapittel 7.2.

Tabell 2 Vurdering av sårbarhet i ulike sektorer basert på de sju faktorene beskrevet over.

Funksjoner / Sårbarhetsfaktorer	Strømforsyning	Digital infrstruktur	Finansielle tjenester	Luftfart	Jernbane	Veitransport
1. Ulike tidskilder	🟡 → 🟢	🟡	🟡	🔴	🟢 → 🟡	🔴
2. Grad av digitalisering	🔴	🔴	🔴	🟡 → 🔴	🟢 → 🔴	🟡
3. Avhengighet av mikrotid	🔴	🔴	🔴	🟡 → 🔴	🟢 → 🟡	🟢
4. Distribuerte systemer	🟡	🟡	🔴	🔴	🟡	🟢 → 🟡
5. Åpne systemer	🟢	🟡	🟢	🟡	🟢 → 🟡	🔴
6. GPS-avhengighet	🔴 → 🟡	🟡	🟡	🔴	🟢 → 🟡	🔴
7. Manglende redundans	🟡 → 🟢	🟢	🟢	🟡	🟢	🔴

🔴 = stor grad 🟡 = moderat grad 🟢 = liten grad

En sirkel viser vurdering av dagens situasjon og to sirkler viser dagens situasjon og forventet utvikling.

7.2 Sårbarhet per sektor

Felles sårbarheter i alle sektorer

Digitalisering

Digitalisering er i økende grad en løsning for å effektivisere tjenester. Dette gjelder særlig integrering av informasjonsteknologi (IT) og operasjonell teknologi (OT), der digitale systemer automatiserer, overvåker og styrer fysiske prosesser. Når IT- og OT-systemer kobles sammen, må de dele en felles og nøyaktig tidsreferanse for at data skal tolkes likt.

Tidsfeil i OT kan få umiddelbare sikkerhetskonsekvenser ved at sanntidsdata, alarmer eller styring blir feil eller utilgjengelig. SCADA-systemer og sensorer er typiske eksempler på OT-enheter som krever tidssynkronisering. Det gjør blant annet strømforsyning og luftfart særlig sårbare for forstyrrelser i tidssignaler.

IT-systemer understøtter databehandling, kommunikasjon og sikkerhet i digitale tjenester. Også disse er avhengige av en felles og nøyaktig tidsreferanse, men tidsfeil gir normalt ikke umiddelbare fysiske konsekvenser. Derimot kan usynkronisert tid få store konsekvenser for tjenester som krever presis tidsstempling av aktiviteter, som transaksjoner og oppgjør i bankvesenet.

Ulike kilder til tid

Kun sentrale virksomheter i to av de seks undersøkte samfunnsfunksjonene brukte en redundant konstellasjon av uavhengige pålitelige tidskilder i dag; Norges Bank og Telenors landsdekkende transmisjonsnett for ekom. Statnett bruker i dag tidssignaler fra GNSS, men planlegger å ta i bruk atomklokker i sitt sentrale styringssystem for kraftforsyning. Innen luftfart og jernbane er det NTP-løsninger med lokale klokkenoder. Innen veisektoren er det foreløpig ingen konkrete planer om å ta i bruk atomklokker. Det er de sentrale aktørene i sektorene som sikres best med nøyaktig tid, mens andre aktører i sektorene bruker ulike og mindre sikre kilder til tid.

Strømforsyning

Kraftsektorens sårbarhet ligger i stor grad av digitalisering, avhengighet av mikrotid og bruk av satellittbasert tid i ytre ledd av systemet. Nøyaktig og synkronisert tid er helt nødvendig for å overvåke balansen i strømnettet, særlig i transmisjonsnettet. Kontrollsentraler mottar tidsstemplet sanntidsdata fra sensorer i transmisjons- og regionalnett, og avvik i tid mellom sensorer og styringssystem kan gi feil styringsinformasjon. Tid hentes i stor grad fra GNSS, og spoofing kan dermed skape tidsavvik som kan tolkes som fasefeil og føre til utkoblinger.

Digital infrastruktur

Elektronisk kommunikasjon er sårbar for tidsfeil på grunn av høy grad av digitalisering og avhengighet av svært nøyaktig tid. Det landsdekkende transportnettet til Telenor har imidlertid tidskilder med god redundans. Felles tidsreferanse er særlig viktig i 5G-nett der nøyaktig tid brukes for å koordinere samtidig datatrafikk. Operatører som bruker GNSS-mottakere på basestasjoner utgjør en sårbarhet både for seg selv og andre operatører i samme dekningsområde.

Finanssektoren

Den største sårbarheten ved tidsfeil i finansielle tjenester er grad av digitalisering og avhengighet av mikrotid. Bankvesenet er imidlertid et relativt lukket system og Norges Bank sentralt har en sikker og redundant løsning for nøyaktig tid. Finanssektoren er svært avhengig av sikker, nøyaktig og synkronisert tid for at IT-systemer skal kommunisere korrekt og gjennomføre transaksjoner i handel, oppgjør og avregning. Avvik på mikrosekund- til millisekundnivå kan føre til at handler ikke godtas. Aktørene benytter ulike tidskilder med varierende GNSS-avhengighet, og det finnes ikke en felles tidsinfrastruktur for bankvesenet.

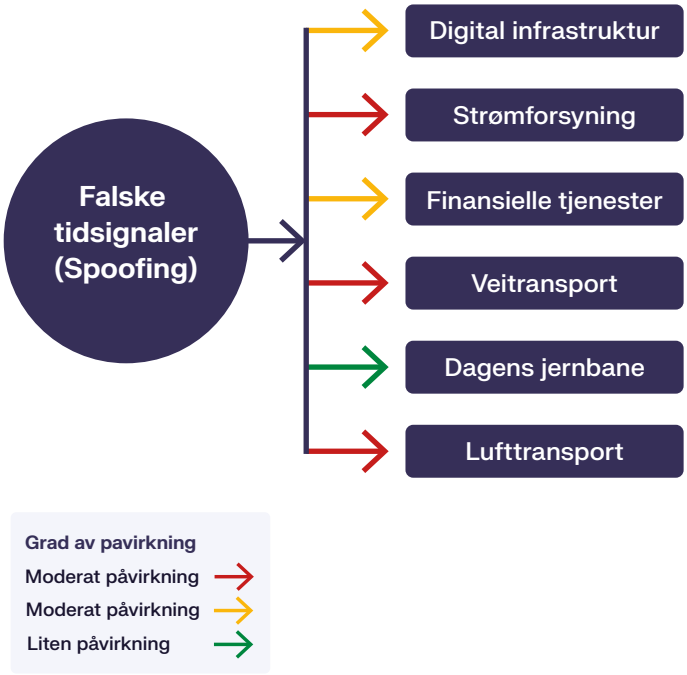
Luftfart
Luftfart har sårbarheter for tidsfeil knyttet til bruk av GPS i flyene og kommunikasjonen som skjer mellom flyene og kontrolltårnet, som får tid fra et internt nettverk i Avinor med atomklokker. Luftfarten er i økende grad basert på digitaliserte systemer for navigasjon, overvåking og kommunikasjon, der både fly og bakkeinfrastruktur er avhengige av nøyaktig og felles tidsreferanse. Satellittbaserte løsninger benyttes som primær kilde til tid og posisjon i flyenes systemer, i overvåking av luftrommet og i digitale kontrolltårn. Sårbarheten øker med innføring av satellittbaserte innflyvningsprosedyrer til erstatning for bakkebasert utstyr.

Jernbane
Jernbanen er i dag lite sårbar mot spoofing. Styring og overvåking fra trafikkstyringssentralene er basert på mekanisk utstyr i togsporene og ikke digital teknologi. Kommunikasjonen mellom sentralene og togførerne skjer over GSM-R, et lukket mobilnett for jernbanen. Etter innføringen av neste generasjons signalsystem (ERTMS), vil togstyring og -overvåking bli mer digitalisert og avhengigheten av nøyaktig tid øke. Distribusjon av tid via eget nettverk med atomklokker, er robust. Med tid fra GPS eller åpent 5G mobilnett i togene, oppstår en mulighet for spoofing.

Veitransport
Veitransporten har sårbarheter for tidsfeil på grunn av bruk av satellittbasert tid både i sentrale systemer og regionale og lokale servere. Elektronisk utstyr langs veiene og i tunneler kommuniserer med vegtrafikk-sentralene gjennom mobilnett og bruker GPS der det ikke er dekning. Datasystemene som brukes i dag er ikke avhengig av mer nøyaktig tid enn millisekunder. Avhengigheten av nøyaktig og synkronisert tid øker imidlertid med «Intelligente transportsystemer» jf. kap. 6.4.

Figuren under illustrerer i hvilken grad de syv sårbarhetsfaktorene i tabell 1 samlet påvirker de seks analyserte samfunnsfunksjonene.

Figur 6: DSBs vurderinger av hvor sårbare seks kritiske samfunnsfunksjoner er for falske tidssignaler fra satellitter (spoofing).



8 Vurdering av samfunns-konsekvenser

Konsekvenser for befolkningen vurderes i form av påvirkning på fem samfunnsverdier, som har stor betydning for samfunnet og befolkningen. Samfunnsverdiene er inndelt i ti konkrete konsekvenstyper. Samfunnsverdiene som vurderes er de samme for alle AKS-analyser som er produsert siden 2010. Framgangsmåten for skåring er beskrevet i Risikoanalyse på samfunnsnivå (DSB 2019).[43]

Tabell 3: Samfunnsverdiene og konsekvenstypene som vurderes i AKS

Samfunnsverdi	Konsekvenstype
Liv og helse	Antall dødsfall
	Antall alvorlige skadde og syke
Natur og kultur	Langtidsskader på naturmiljø
	Uopprettelige skader på kulturmiljø
Økonomi	Direkte økonomiske tap
	Indirekte økonomiske tal
Samfunnsstabilitet	Sosiale og psykologiske reaksjoner
	Påkjenninger i dagliglivet
Demokratiske verdier og styringsevne	Tap av demokratiske verdier og nasjonal styringsevne
	Tap av kontroll over territorium

8.1 Forutsetninger og usikkerhet i konsekvensvurderingene

I usikkerhetsvurderingene vurderer vi kunnskapsgrunnlaget som vurderingene av sannsynlighet og konsekvenser bygger på. Svak kunnskap gir større usikkerhet i vurderingene enn sterk kunnskap. Resultatenes følsomhet overfor endringer i forutsetningene (sensitivitet) bidrar også til usikkerhet.

I vurderingene har vi forutsatt en varighet av forstyrrelsene på rundt en uke for hver kritiske samfunnsfunksjon. Det betyr en antakelse om at det går en uke fra GNSS-mottakeren blir utsatt for spoofing og datasystemer begynner å feile, til tidsfeilen er rettet og systemene fungerer normalt igjen. Varigheten av hendelsene er avgjørende for omfanget av konsekvenser. I scenarioet blir de ulike funksjonene spoofet hver for seg over en lengre periode og vurderes ikke som en samtidig hendelse.

Det finnes mange typer GNSS-mottakere med ulik evne til å oppdage og avvise falske signaler (firewalls). Erfaringer fra Jammertesten på Andøya viser at mottakere kan reagere ulikt på samme falske signal[44]. Vi antar at GNSS-mottakere i kritiske samfunnsfunksjoner er relativt robuste, men med stor variasjon bl.a. avhengig av alder.

43 DSB: Risikoanalyse på samfunnsnivå

44 Av flere mulige responser på spoofing, kan en GNSS-mottaker låse seg på et falskt signal og begynne å avvise de ekte signalene. GNSS-mottakere kan også slutte å fungere permanent.

Spoofing av tidssignaler har både direkte og indirekte konsekvenser. De direkte konsekvensene er påvirkningen på kritiske samfunnsfunksjoner, mens det er svikt i disse som påvirker befolkningen. Det er altså en dobbelt usikkerhet i konsekvensvurderingene for samfunnet som helhet.

Vi har lite erfaring med omfattende spoofing-angrep, dette øves ikke i praksis[45] og kunnskapen om spoofing som fenomen er mangelfull. Spoofing er en ulovlig aktivitet og opplysninger om mulige rekkevidder for spoofing varierer fra noen titalls meter til 50 km. Det er også lite kunnskap i sektorene om hvordan ulike systemer påvirkes, og hvordan feil forplanter seg til andre systemer. Det gir et stort utfallsrom for mulige konsekvenser.

8.2 Liv og helse

Mulige dødsfall som følge av falske tidssignaler kan knyttes til forstyrrelser av basestasjoner, som kan ramme telefoner om akutt hjelpebehov til nødsentralene og nødnett. Også feil i satellittbaserte navigasjonssystemer kan i verste fall føre til fatale ulykker med dødsfall. Antall dødsfall vurderes til å kunne ligge i intervallet 6-20, noen som tilsvarer «små konsekvenser» i AKS-sammenheng.

Det kan også forventes et antall alvorlig skadde og syke pga. forsinket akutthjelp og ulykker i luftfart. I tillegg kan reduserte muligheter for overvåking og styring av veitrafikken fra Vegtrafikksentralene, føre til trafikkulykker. Vi anslår at det vil ligge i intervallet 21-100 personer og innebærer «små konsekvenser» i AKS-sammenheng.

Spoofing direkte av helsesystemer eller Nødnett inngår ikke i denne analysen.

Natur og kultur
Ingen direkte konsekvenser av scenarioet.

8.3 Økonomi

Beregningene av økonomiske tap er støttet av kunstig intelligens. De er basert på forutsetninger fra scenarioet og konsekvensvurderingene, og tilgjengelig kildegrunnlag for kostnader og priser. Tallene bør tolkes veiledende, og bør kvalitetssikres ved bruk i egen sektor. Av hensyn til etterprøvbarhet og ev. videre bearbeiding av tallmaterialet i egen sektor, er modellene og kildegrunnlaget dokumentert i vedlegg 3.

Strømforsyning: I kraftsektoren kommer de direkte kostnadene av ekstra bemanning, feilretting ute i nettet og arbeid for å få systemene i takt igjen. Disse er anslått til 50–140 millioner kroner. De indirekte kostnadene blir ofte større, fordi gjentatte korte strømbrudd gir produksjonstap i bedrifter og praktiske problemer i husholdninger. De er anslått til 40 millioner-1,92 milliarder kroner

Luftfart: I luftfarten er de direkte kostnadene knyttet til innstilte fly, omdirigeringer, ekstra bemanning og teknisk opprydding. Disse er anslått til 240–700 millioner kroner. De indirekte kostnadene er størst: folk kommer for sent fram, arbeidsreiser faller bort, og leveranser stopper opp. Disse er anslått til 1,0–2,9 milliarder kroner.

Vei: I veisektoren er direkte kostnader blant annet ekstra drift i trafikkstyringen, mer patruljering og midlertidige sikkerhetstiltak. Disse er anslått til 45–130 millioner kroner. Indirekte kostnader kommer fra mer kø, lengre reisetid, omkjøringer og forsinkede leveranser. De er anslått til 60–394 millioner kroner.

Digital infrastruktur: For mobil- og datatjenester er direkte kostnader knyttet til intensiv feilretting og

45 Bortsett fra begrenset testing under jammer-øvelsene på Andøya.

ekstra kundehåndtering, anslått til 35–110 millioner kroner. Indirekte kostnader oppstår når nettet blir tregt eller ustabilt: folk og virksomheter bruker mer tid, betaling og bestillinger går tregere, og arbeid stopper opp i perioder. Disse er anslått til 180 millioner-1,12 milliarder kroner.

Jernbane: I jernbanen er direkte kostnader knyttet til ekstra bemanning, manuell styring og teknisk opprydding, anslått til 35–110 millioner kroner. Indirekte kostnader kommer av innstillinger, forsinkelser, og problemer for godstransporten. Disse er anslått til 174 millioner-1,31 milliarder kroner.

Finans: I finanssektoren er direkte kostnader knyttet til krisehåndtering, kontroll av transaksjonsdata, teknisk opprydding og regelverksarbeid, anslått til 70–430 millioner kroner. De indirekte kostnadene blir større: tregere handel, forsinkelser i oppgjør, mer bundet kapital og lavere aktivitet i markedet. Disse er anslått til 420 millioner-3,3 milliarder kroner.

Samlede direkte kostnader knyttet til scenarioet er beregnet til å være mellom 475 og 1 620 mill.kr. Det innebærer «middels store» direkte økonomiske tap i AKS-sammenheng (0,5-2 mrd. kr).

Samlede indirekte kostnader er beregnet å ligge mellom 1 870 og 10 900 mill. kr. Det innebærer «store» indirekte økonomiske tap i AKS-sammenheng (2-10 mrd. kr).

8.4 Samfunnsstabilitet

Sosiale og psykologiske reaksjoner

Regionale bortfall av strømforsyning og mobildekning (5G) i en uke, vil skape bekymring og frustrasjon. Stabil strømforsyning blir tatt som en selvfølge. Selv om mange har en viss egenberedskap, er det ikke fullgode reserveløsninger for varme og matlaging. Ingen kan love når strømmen og mobilnettet er tilbake, og folk etterspør nødløsninger fra kommunene. Mange kommer seg ikke på jobb i strømløse bygninger og skoler og barnehager må stenge. I praksis stopper det meste opp i en uke, mens folk er opptatte av å finne måter å klare seg på hjemme.

Myndighetene har ingen gode forklaringer på hva som er årsaken til problemene. Det virker som at så fort et problem er løst, så dukker det opp et nytt. Statsministeren sier at man ikke kan utelukke at Norge er utsatt for hybride angrep mot infrastrukturen og at det kan komme nye hendelser. Alvoret i situasjonen preger befolkningen og skaper både sosial uro og mobilisering.

For å vurdere styrken av «sosiale og psykologiske reaksjoner», skal følgende kjennetegn vurderes: Ukjent hendelse, rammer sårbare grupper, tilsiktet hendelse, manglende mulighet til å unnslippe, forventningsbrudd, manglende mulighet til å håndtere hendelsen og at hendelsen rammer tilfeldig. Scenarioet har alle disse kjennetegnene og konkvensene vurderes som «svært store» i AKS-sammenheng.

Påkjenninger i dagliglivet

Omfang og varighet av svikt i strømforsyningen, svikt i andre kritiske samfunnsfunksjoner og behov for evakuering, vurderes for denne konsekvenstypen.

Spoofing-angrepene i scenarioet vil i første omgang merkes i befolkningen i form av regionale strømbrudd, bortfall av mobilnett i områder og stedvise forsinkelser i luft-, jernbane og veitrafikk. Dette vil igjen få følgehendelser. Uten strøm må butikker og energistasjoner stenge og betaling med mobil kan ikke gjennomføres uten dekning. Det blir vanskelig å skaffe mat og drivstoff. Kjøleaggregater, drivstoffpumper, signalanlegg for tog og veitrafikk vil slutte å fungere. Hele varetransportkjeden er avhengig av nettbaserte systemer, og det vil oppstå store forsinkelser i vareleveranser. I veitrafikken blir mange tunneler stengt og fører til omkjøringer og forsinkelser.

Spoofingen av kritiske samfunnsfunksjoner vil ramme et stort antall innbyggere. Ubalanse i transmisjonsnettet og utkopling av f.eks. tre store nettselskaper, kan ramme 300 000 abonnenter. Reserveløsninger for tilførsel av kraft til disse områdene (øydrift), kan redusere antall strømløse til 150 000 abonnenter. Forstyrrelser i øvrige samfunnsfunksjoner antas å ramme omtrent like mange. Varigheten er forutsatt i scenarioet å være en uke.

Utsatte grupper som kan få behov for evakuering, er bl.a. innbyggere som kun har elektrisk oppvarming og syke som er avhengige av elektroniske hjelpemidler eller medisinsk utstyr til behandling hjemme. Behovet for evakuering vil avhenge av årstid, men kan ligge på 100-1000 personer.

Samlet sett vurderes omfanget av påkjenninger i dagliglivet som «store» i AKS-sammenheng.

8.5 Demokratiske verdier og styringsevne

Kritiske funksjoner som både befolkningen og næringslivet er avhengige av, blir rammet. Forstyrrelsene er imidlertid avgrensede i både tid og geografisk omfang. De fordekte angrepene begrenser til en viss grad handlefriheten og styringsevnen, og oppleves som en trussel mot demokratiske verdier. Konsekvensene vurderes som «små» i AKS-sammenheng.

Forsøk fra en fremmed stat på å svekke og destabilisere det norske samfunnet, er en krenkelse av landets selvstendighet, sikkerhet og integritet. Spoofing-angrepene er en type ikke-militær virkemiddelbruk som fører til tap av nasjonal kontroll over kritiske samfunnsfunksjoner, men ikke tap av territorium. Tapet av kontroll er kortvarig, men usikkerheten angrepene medfører er langvarig. Konsekvensene vurderes som «middels store» i AKS-sammenheng.

8.6 Oppsummering av risiko knyttet til scenarioet

Under er en skjematisk fremstilling av vurderingene av sannsynlighet og konsekvenser basert på en femdelt skala fra svært små til svært store.

Sannsynlighetsvurdering						
		Svært lav	**Lav**	**Middels**	**Høy**	**Svært høy**
Sannsynlighet for scenarioet			○			
Sannsynlighet for et generalisert scenario				○		
Konsekvensvurdering						
Samfunnsverdi	**Konsekvenstype**	**Svært små**	**Små**	**Middels**	**Store**	**Svært store**
Liv og helse	Dødsfall		○			
	Alvorlige skadde og syke		○			
Natur og kultur (ikke relevant)	*Langtidsskader på naturmiljø*	*Ikke relevant*				
	Uopprettelige skader på kulturmiljø	*Ikke relevant*				
Økonomi	Direkte økonomiske tap			○		
	Indirekte økonomiske tap				○	
Samfunnsstabilitet	Sosiale og psykologiske reaksjoner					○
	Påkjenninger i dagliglivet				○	
Demokratiske verdier og styringsevne	Tap av demokratiske verdier og styringsevne		○			
	Tap av nasjonal kontroll over samfunnsfunksjoner			○		
Samlet vurdering av konsekvenser					○	
		Svært liten	**Liten**	**Moderat**	**Stor**	**Svært stor**
Samlet vurdering av usikkerhet	Kunnskapsgrunnlag og sensitivitet				○	

I kapittel 5 forklarer vi hvordan sannsynligheten for scenarioet er vurdert.

9 Forslag til tiltak

Selv om det påpekes sårbarhet og risiko knyttet til bruk av satellittbasert tid i analysen, er det ingen enkle tiltak som kan løse problemet. Bruk av satellittbaserte tidssignaler og særlig GPS, er så utbredt at alle sektorer er avhengige av at de gir riktig tid. GPS er enklere og rimeligere å bruke enn alternative tidskilder. Dessuten har GPS fungert godt i over 30 år, så hvorfor løse et problem man ikke har. Første skritt for å vurdere tiltak, er å forstå problemet og det er dette vår analyse håper å gi et bidrag til.

Tiltakene vi foreslår under er ikke ferdig utredede tiltak, men tiltak vi mener det er verdt å vurdere.

Kort sikt

- Sette krav til at alle mobiloperatører må ha basestasjoner som er robuste mot spoofing av satellittbaserte tidssignaler.
- Kritiske samfunnsfunksjoner som bruker NTP-tid bør undersøke hvordan dette nettverket er satt opp og om det har en autorativ pålitelig tidskilde, som Justervesenets tidstjeneste eller atomklokker. Frivillige NTP-pooler gir ikke dokumenterbar og sikker tid, og er satt sammen av tjenere som kan ha direkte avhengigheter til GPS.
- Ved bruk av flere tidskilder, bør svært stabile atomklokker være den primære tidskilden og satellittbasert tid den sekundære.
- Kritiske samfunnsfunksjoner bør etterspørre en pålitelig tidstjeneste fra datasentre de har servere i (atomklokker, nasjonal tidstjeneste eller et pålitelig NTP-nettverk). Mange brukere med hver sine GNSS-mottakere på datasentre kan gjøre datasentre mer utsatte for spoofing.
- Kritiske samfunnsfunksjoner bør anskaffe mottakere som kan bruke signaler fra flere satellittsystemer (minimum amerikanske GPS og europeiske Galileo).
- Virksomheter bør kartlegge sine avhengigheter av satellittbaserte tidssignaler og teste hvordan systemene reagerer på tidsavvik.

Lengre sikt

- Etablere en nasjonal tidstjeneste knyttet til UTC-samarbeidet. Det blir vil gi nøyaktig, sikker og sporbar tid til virksomheter som knytter seg til tjenesten enten via fiber eller et riktig oppsatt NTP-nettverk.[46]
- Gjennomføre en samfunnsøkonomisk analyse av å etablere Loran-stasjoner (eLoran) i Norge (bakkebaserte PNT-sendere). Senderne kan fungere som backup for tidsreferanse og posisjon, hvis GNSS-systemene feiler.

Oppfølging av disse tiltakene hviler i første rekke på Justervesenet og Nasjonal kommunikasjonsmyndighet (Nkom), og deres overordnede departementer Digitaliserings- og forvaltningsdepartementet (DFD) og Nærings- og fiskeridepartementet (NFD).

46 Ref. omtale i kapittel 2

Vedlegg 1: Begrepsliste

Tid – presisjon, nøyaktighet og stabilitet

- En klokke er nøyaktig hvis den viser **riktig** tid i forhold til UTC.
- En klokke er presis om den tikker **konsistent**, for eksempel alltid går fem sekunder for fort.
- En klokke er stabil hvis den **holder takten** lenge uten å drifte, altså hvor lite gangfarten til klokken endrer seg over tid.

GNSS

Global Navigation Satellite System, eller *globale navigasjonssatellittsystemer*, er en fellesbetegnelse på alle satellittbaserte systemer som leverer signaler for posisjonering, navigasjon og tid (PNT). GPS (USA), Galileo (EU), GLONASS (Russland) og BeiDou (Kina) er slike systemer. GPS er ett av flere slike systemer.

«System»-begrepet i denne sammenhengen viser til at flere tekniske og organisatoriske ledd må samarbeide for at en satellittbasert tjeneste skal fungere. GNSS deles typisk inn i tre segmenter:

- *Romsegment:* Selve satellittene i bane rundt jorden, utstyrt med presise klokker og signalsendere.
- *Bakkesegment:* Kontrollstasjoner og bakkebasert infrastruktur som overvåker, kontrollerer og korrigerer satellittenes baner og tidssignaler.
- *Brukersegment:* Alt utstyr og alle aktører som mottar og utnytter GNSS-signaler – enten direkte gjennom mottakerutstyr (GPS på høyfjellet) eller indirekte gjennom bruk av tjenester som benytter satellittsignaler til drift.

Kort illustrert: Satellittene i verdensrommet (*romsegmentet*) trenger overvåkning, styring og tidvis korrigering fra bakkestasjoner (*bakkesegmentet*), slik at de kan sende ut pålitelige signaler til brukere, f.eks. til navigasjon på høyfjellet eller tidssynkronisering av IT-servere (*brukersegmentet)*.

PNT

PNT står for *posisjonsangivelse, navigasjon og tidsangivelse*. Dette er tre funksjoner som beskriver evnen til å:

- Bestemme et sted (posisjon)
- Beregne fart og retning (navigasjon)
- Angi nøyaktig tid (tidsangivelse)

Navigasjonssatellitter (GNSS) er bærere av teknologi for signaler som gir PNT. Satellittene gir global dekning fordi de er langt fra jorden, høy presisjon fordi de har atomklokke, og lav kostnad fordi signalene brukes på bakken ved hjelp av rimelige mottakere.

Fordi navigasjonssatellitter er utstyrt med atomklokke som synkroniseres mot et felles tidssystem på jorden, brukes tidssignalene av virksomheter som behøver presis tid til tidssynkronisering av f.eks. operasjonell teknologi (kraftnett) og informasjonssystemer (servere og nettverk).

I sum har dette medført at tilnærmet alle offentlige og private tjenester eller infrastruktur som krever posisjons- eller tidsinformasjon, har en avhengighet til GNSS. PNT kan også leveres gjennom bakkebaserte radiosystemer som Loran-C eller eLoran, men slike løsninger er i liten grad operative i dag.

Blokkere signaler - Jamming

Jamming fører til støy i frekvensbåndet slik at mottakere ikke får inn noen signaler, og mister f.eks. muligheten til å navigere elektronisk.

Prinsippet bak jamming er at en radiosender sender ut støy på samme frekvenser som brukes av navigasjonssatellitter. Fordi signalene fra GNSS-satellitter er svært svake når de når jordoverflaten – ofte sammenlignet med termisk bakgrunnsstøy – kreves det lite energi for å overdøve signalene lokalt. Alle GNSS-systemer opererer dessuten i nærliggende frekvensbånd (typisk L-båndet), noe som gjør at jamming ofte påvirker flere satellittsystemer samtidig innenfor samme område.

Manipulere signaler - Spoofing

Spoofing fører til at mottakere får inn kunstige signaler fra en annen sender med villedende informasjon om posisjon og tid.

Spoofing er en mer avansert form for signalforstyrrelse, der en radiosender bevisst etterligner ekte GNSS-signaler, men med falsk posisjons- eller tidsinformasjon. Spoofing-signalet sendes gjerne med høyere styrke enn de ekte satellittsignalene, slik at GNSS-mottakeren prioriterer det forfalskede signalet. Resultatet er at mottakeren beregner feil uten nødvendigvis å oppdage at noe er galt.

Et eksempel er et maritimt fartøy som ved hjelp av spoofing manipuleres til å tro at det befinner seg i Bergen, mens det i virkeligheten seiler langs sørlands-kysten. Spoofing krever mer avansert utstyr og teknisk kompetanse enn jamming, og er vanskeligere å oppdage fordi signalene tilsynelatende er «gyldige», selv om de er falske. I praksis kan spoofing derfor forveksles med datafeil eller cyberangrep.

Gjenbruke signaler - Meaconing

Meaconing fører til at mottakere får inn ekte satellitt-signaler med forsinkelse fra en annen sender, som skaper feilberegninger.

Meaconing innebærer at ekte GNSS-signaler brukes på nytt ved å sendes ut fra en annen posisjon enn der de først ble mottatt – ofte med en liten forsinkelse. Dette fører til at GNSS-mottakere tolker signalene feil, og dermed beregner unøyaktig posisjon eller tid.

Dette gjør meaconing vanskelig å oppdage, fordi det ikke nødvendigvis oppstår signalbrudd eller åpenbare avvik. Et praktisk eksempel kan være en drone som lures til å tro at den fortsatt befinner seg innenfor et godkjent operasjonsområde, fordi den mottar gjen-brukte signaler fra et annet sted.

Vedlegg 2: Registrerte spoofing-hendelser

Under er et utvalg rapporterte GNSS-spoofing-hendelser med kildehenvisninger 2022–2025.

1) Østersjøen / Baltikum – statlig elektronisk krigføring og sanksjonsomgåelse (2024–2025)

- Tankskip som spoofet AIS/GNSS-posisjon for å skjule anløp til russiske havner (Gulf of Finland, 2024)
- Skip fremstod på kart som om de var andre steder
- Koblet til russisk sanksjonsomgåelse og beskyttelse av oljeeksport

Finske myndigheter observerte at flere tankere «spoofet» posisjonene sine for å skjule besøk til Russland (Reuters).

2) Luftfart over Baltikum og Øst-Europa – massiv spoofing av fly (2023–2025)

- Tusenvis av fly påvirket av falske GNSS-posisjoner
- Spesielt nær Kaliningrad, Belarus og russiske områder
- Fly rapporterte falske terrengvarsler og navigasjonsfeil

Rundt 46 000 hendelser ble rapportert mellom august 2023 og mars 2024 (Business Insider).

3) Massespoofing av skip i Østlige Middelhav (2024)

- Store grupper skip fikk identisk falsk posisjon
- Eksempel: Over 100 fartøy samtidig «flyttet» til Beirut-området
- Klassisk signatur på koordinert spoofing (ikke AIS-manipulasjon alene)

En hendelse involverte 117 skip som ble forskjøvet til Beirut Airport-området, senere over 200 fartøy (GPSPATRON).

4) Red Sea / Bab el-Mandeb – navigasjonsulykker knyttet til spoofing (2024–2025)

- GNSS-spoofing bidro til grunnstøting av handelsskip
- Kritisk chokepoint for global handel

Containerskipet MSC Antonia gikk på grunn i mai 2025 etter spoofing. (SAFETY4SEA)

Flere hendelser og kollisjoner er rapportert i samme område. (SAFETY4SEA)

5) Svartehavet / Krim – fly «teleportert» til falske flyplasser (2024–2025)

- Fly fikk posisjon «låst» til områder i russisk-kontrollert Krim
- Klassisk statlig spoofing-teknikk for luftromsbeskyttelse

Spoofede posisjoner hoppet ofte til Simferopol-området (Spire: Global Data and Analytics).

6) Europa generelt – systematiske hendelser knyttet til Ukraina-krigen (2022–2025)

- Over 80 betydelige hendelser dokumentert i europeisk luft- og sjøtrafikk
- Ofte attribuert til russiske militære sendere

Hendelsene påvirket flyruter, skip og transportkorridorer (Starburst).

EU-land rapporterer kraftig økning i interferens-tilfeller siden Russlands invasjon av Ukraina (Defence Industry and Space).

Vedlegg 3: Beregning av økonomiske tap

Av hensyn til etterprøvbarhet og videre undersøkelser i egen sektor, er grunnlaget for beregningene og kilder for verdier dokumentert her.

1.1 Verdi av tid (personer)

- **Brukt i modeller:** 220–700 kr/time avhengig av sektor og reiseformål.
- **Kildegrunnlag:** Norsk verdsettingsstudie (TØI 1762/2020) + implementering i transportmodeller/ V712. (Transportøkonomisk institutt)
- **Begrunnelse:**
  - Lavere verdi i daglig/ikke-forretningskritisk mobilitetsfriksjon.
  - Høyere verdi i luftfart/tjenestereiser (høy andel arbeidstid/tapt produksjon).

Verdi av tid (næring/arbeidstid)

- **Brukt:** 600–1 500 kr/time (sektoravhengig).
- **Kilder:** TØI/V712 for tidsverdier + tidsavhengige kostnader for tungtrafikk i V712 (bl.a. ~754 kr/time for lastebil i 2020-kr) som nedre anker for logistikk/ tungtransport. (Statens vegvesen[47])
- **Begrunnelse:**
  - 600 kr/time brukt som konservativ «produktiv arbeidstid»-sats i ekom/vei.
  - Høyere i luftfart/finans når konsekvens gjelder høyt verdiskapende transaksjons-/beslutningstid.

Kraftavbrudd – kundekostnader

- **Brukt:** Hushold 100–150 kr/kunde-time, næring 800–1 500 kr/kunde-time (i revidert kraftmodell).
- **Kildegrunnlag:** NVE/RME anbefaler KILE som hovedregel for prising av forsyningssikkerhet/ avbruddskostnader. (Veiledere NVE)
- **Begrunnelse:** Intervallene er holdt i størrelses-orden som forenklede scenarioverdier når konkrete KILE-funksjoner ikke var lagt inn i modellen.
- **Finanssystem volum (NBO)**
- **Brukt:** 350 mrd kr/dag, 4 600 oppdrag/dag, rundt 100+ deltakere.
- **Kilde:** Norges Bank årsrapport 2024 og Finansiell infrastruktur 2025 / daglige nøkkeltall. (Norges Bank)

47 925 kroner i 2025, omgjort med Norges Banks inflasjonskalkulator.

Strømforsyning

Forutsetninger[48]

Parameter	Lav	Høy	Kommentar
Region (kunder totalt)	600 000	1 000 000	hushold + næring
Hendelser/døgn (lokale utkoblinger)	5	15	av-og-på
Berørte kunder pr hendelse	10 000	50 000	lokalitet
Varighet pr hendelse	15 min	45 min	minutter–timer
Andel næringskunder (i berørt mengde)	10%	10%	enkel fordeling
Kostnad pr kunde-time hushold	100 kr	150 kr	komfort/tidsbruk
Kostnad pr kunde-time næring	800 kr	1 500 kr	produksjon/drift

1) Direkte økonomiske tap

Kostnadskomponent	Sum (lav–høy)
Kontrollsentral: ekstra bemanning/overvåkning	15–40 mill.
Feilanalyse (PMU/RTU), OT/IKT, re-synk	20–60 mill.
Utrykning + beredskapstiltak	15–40 mill.
Sum direkte tap	**50–140 mill.**

2) Indirekte økonomiske tap (kunde-timer)

Først beregnes «kunde-timer» i perioden:

- **Lav:** 5 × 10 000 × 0,25 t × 7 = **87 500 kunde-timer**
- **Høy:** 15 × 50 000 × 0,75 t × 7 = **3 937 500 kunde-timer**

Deretter prises med ulike satser for hushold og næring.

Komponent	Lav	Høy
Hushold (90% av kunde-timer)	~7,9 mill.	~531 mill.
Næring (10% av kunde-timer)	~7,0 mill.	~591 mill.
Særskilt industrifriksjon (der relevant)	25 mill.	800 mill.
Sum indirekte tap	**≈ 40 mill.**	**≈ 1 920 mill.**

48 Kostnader ved ikke-levert strøm hentet fra NVE/KILE.

3) Total – kraft

Type tap	Intervall
Direkte	50–140 mill.
Indirekte	40–1 920 mill.
Total (7 døgn)	**90 mill. – 2,06 mrd. kr**

Jernbane

Forutsetninger[49]

Parameter	Lav	Høy	Kommentar
Geografisk omfang	1 stor korridor + knutepunkt	2–3 korridorer	ERTMS nivå 2 i drift der hendelsen slår inn
Varighet	7 døgn	7 døgn	av-og-på
Teknisk effekt	Kjøretillatelser forsinkes/avvises periodisk	Hyppige «safe state»-overganger	ikke bortfall av sikkerhets-marginberegning
Trafikal effekt	redusert hastighet + periodiske stans	lavere kapasitet + flere innstillinger	sikkerhet opprettholdes
Berørte tog per døgn	300	700	persontog + noe gods
Inntekts-/driftsrelevante personturer per døgn	120 000	280 000	berørte reiser
Andel innstilte tog	5 %	15 %	konkrete volumer, ikke faktor
Andel kraftig forsinkede tog	25 %	45 %	av gjenværende tog
Snitt forsinkelse, forsinket tog	20 min	60 min	
Verdi av tid passasjer	220 kr/t	300 kr/t	konservativ transportverdi
Berørte godstog per døgn	20	70	i berørte korridorer
Kostnad per berørt godstog (drift/terminal/venting)	30 000 kr	120 000 kr	konkret logistikkledd

49 Jernbaneøkonomisk metode/verdsetting: Jernbanedirektoratet

1) Direkte økonomiske tap

Kostnadskomponent	Enhet	Lav	Høy	Sum
Ekstra bemanning trafikkstyring/signal	fast (7 døgn)	12 mill.	35 mill.	12–35 mill.
Feilsøking/re-synkronisering (NTP, klokkenoder, ETCS-grensesnitt)	fast	10 mill.	30 mill.	10–30 mill.
Hendelseshåndtering/beredskap og manuelle prosedyrer	fast	8 mill.	25 mill.	8–25 mill.
Midlertidige operative tiltak på stasjoner/knutepunkt	fast	5 mill.	20 mill.	5–20 mill.
Sum direkte tap				**35–110 mill.**

2) Indirekte økonomiske tap

2a) Passasjerer – tapt tid og innstillinger (konkret volum)

Beregning per døgn:

- Berørte turer: 120 000 - 280 000
- Innstilte tog påvirker en andel turer; disse gis høy tidsulempe (omvei/innstilling).
- Forsinkede tog gir tidsulempe iht. snittforsinkelse.

Forenklet samlet resultat (7 døgn):

Komponent	Lav	Høy
Tapt passasjertid/verdiskaping	~140 mill.	~1 050 mill.

2b) Gods – logistikk- og produksjonsfriksjon (konkret volum)

Parameter	Lav	Høy
Berørte godstog per døgn	20	70
Kostnad per berørt godstog	30 000 kr	120 000 kr
7 døgn	**4 mill.**	**59 mill.**

I tillegg legges et konkret tillegg for terminal-/omlastingsfriksjon i knutepunkt:

Tilleggspost	Lav	Høy
Terminal-/omlastingsfriksjon	10 mill.	80 mill.

Sum godsrelatert indirekte tap: 14–139 mill.

2c) Operasjonell ettervirkning

Tog og materiell «ute av rute», mannskapsbinding, gjenoppretting av ruteplan er en egen post:

Post	Lav	Høy
Ettervirkningskost (7-døgns hendelse)	20 mill.	120 mill.

Sum indirekte tap

Komponent	Sum
Passasjerer	140–1 050 mill.
Gods/terminal	14–139 mill.
Ettervirkning	20–120 mill.
Sum indirekte tap	**174–1 309 mill.**

3) Samlet økonomisk konsekvens – jernbane

Type tap	Intervall
Direkte tap	35–110 mill.
Indirekte tap	174–1 309 mill.
Total (7 døgn)	**209 mill. – 1,42 mrd. kr**

Luftfart

Forutsetninger[50]

Parameter	Lav	Høy	Kommentar
Innenlands flyginger	1 100/døgn	1 100/døgn	400 000/år
Varighet	7 døgn	7 døgn	av-og-på
Kanselleringsandel	10%	20%	konsekvens av redusert kapasitet/manuell drift
Forsinkelsesandel (av *gjenværende* flyginger)	25%	40%	store forsinkelser
Snitt passasjerer/flyging	120	120	avrundet
Tapt tid pr kansellert passasjer	8 t	10 t	ombooking/overnatt
Tapt tid pr forsinket passasjer	3 t	4 t	2–6 t typisk
Verdi av tid (vektet)	650 kr/t	700 kr/t	blanding privat/næring

50 Tidsverdi per passasjer er basert på dokumentasjonsrapporten til Verdsettingsstudien 2020. Kostnad per kansellert flyvning og omdirigeringskost er ikke dokumentert, og bør vurderes nærmere.

Avledede volumer

- Totalt antall flyvninger i perioden: 1 100 × 7 = **7 700**
- Kansellerte flyvninger: **770 – 1 540**
- Sterkt forsinkede flyvninger: **1 733 – 2 464**

1) Direkte økonomiske tap

Definisjon: «Kost per kansellert flyvning» inkluderer passasjerhåndtering/ombooking, crew/rotasjon og operativ håndtering. Derfor føres ikke disse separat.

Kostnadskomponent	Enhet	Lav	Høy	Sum
Kansellerte flygninger (pakke-kost)	770–1 540 flygninger	150 000 kr	250 000 kr	115–385 mill.
Omdirigeringer (utvalgte flyginger)	70–250 stk	80–150 000 kr	80–150 kkr	6–38 mill.
ATM/flyplass: overtid, manuell drift, ekstra bemanning	fast	60 mill.	140 mill.	60–140 mill.
Teknisk feilsøking/FMS-reset/operativ verifikasjon	fast	60 mill.	140 mill.	60–140 mill.
Sum direkte tap				**240–700 mill.**

2) Indirekte økonomiske tap

2a) Passasjertid[51]

Komponent	Lav	Høy
Kansellerte passasjerer	770×120 = 92 400	1 540×120 = 184 800
Forsinkede passasjerer	1 733×120 = 207 900	2 464×120 = 295 700
Tapt tid (timer)	92 400×8 + 207 900×3	184 800×10 + 295 700×4
Verdi av tid	650 kr/t	700 kr/t
Tapt verdiskaping (7 døgn)	**886 mill. kroner**	**≈ 2 122 mill. kroner**

51 Beregnet direkte fra volumer over

2b) Verdikjede-/logistikkfriksjon

Dette er konkrete tap som ikke fanges fullt av «tapt tid»: avlyste inspeksjoner, avbrutte leveranser av tidskritisk gods, tapte oppdrag osv.

Post	Lav	Høy
Nærings-/logistikkfriksjon	150 mill. kroner	800 mill. kroner

Sum indirekte tap: 1,0 mrd. kroner - 2,9 mrd. kroner

3) Total økonomisk konsekvens – luftfart

Type tap	Intervall
Direkte tap	0,24–0,70 mrd. kr
Indirekte tap	1,0–2,9 mrd. kr
Total (7 døgn)	**1,2–3,6 mrd. kr**

Veitransport

Forutsetninger[52]

Parameter	Lav	Høy	Kommentar
Kjøretøy/døgn (region)	250 000	250 000	stor VTS-region
Andel næring	15%	15%	tung + lett
«Baseline» ekstra reisetid pga degradert styring/info	3 min	10 min	uten multiplikator
Tunnel-/korridorstenginger pga manglende VTS-funksjon	5/døgn	20/døgn	konkret mekanisme
Berørte kjøretøy pr stenging	3 000	8 000	kø/omvei
Ekstra tid pr berørt kjøretøy	20 min	40 min	omvei/kø
Verdi av tid privat/næring	250/600 kr/t	250/600 kr/t	som før

1) Direkte økonomiske tap

Kostnadskomponent	Sum (lav–høy)
Ekstra bemanning VTS + manuell drift	10–25 mill.
Patruljering/entreprenørinnsats	15–40 mill.

52 Statens vegvesen veileder for konsekvensanalyser

Kostnadskomponent	Sum (lav–høy)
Sikringstiltak/lokale stenginger	5–15 mill.
Feilsøking/reset vegutstyr + IKT	15–50 mill.
Sum direkte tap	**45–130 mill.**

2) Indirekte økonomiske tap

Tapt tid beregnes som (baseline for alle) + (ekstra ved konkrete stenginger), fordelt på privat/næring.

Komponent	Lav	Høy
Baseline tidskost (alle kjøretøy)	~26 mill.	~88 mill.
Stengingskost (konkrete hendelser)	~11 mill.	~226 mill.
Næringsmessig «leveransefriksjon» (ikke bare tid)	20 mill.	80 mill.
Sum indirekte tap	**≈ 60 mill.**	**≈ 394 mill.**

3) Total – veitransport

Type tap	Intervall
Direkte	45–130 mill.
Indirekte	60–394 mill.
Total (7 døgn)	**105–524 mill.**

Digital infrastruktur

Forutsetninger[53]

Parameter	Lav	Høy	Kommentar
Region	1,0 mil	1,5 mil	storbyregion
Effekt	5G ustabilt, fallback til 4G	5G ofte ned, 4G overbelastet	fiber upåvirket
Berørte privatbrukere (reelt rammet)	500 000	900 000	de som bruker mobilnett aktivt
Tapt effektiv tid pr privatbruker/dag	5 min	15 min	treghet/feil
Berørte næringsbrukere	120 000	250 000	felt/arbeidsflate/betaling
Tapt effektiv tid pr næringsbruker/dag	10 min	30 min	
Verdi av tid privat/næring	250/600 kr/t	250/600 kr/t	

1) Direkte økonomiske tap

Kostnadskomponent	Sum (lav–høy)
Ekstra drift/NOC, feilsøking, re-synk	25–70 mill.
Midlertidige konfig-/nettverkstiltak	5–15 mill.
Kundetrykk/support	5–20 mill.
Koordinering mot Nkom/myndigheter	2–5 mill.
Sum direkte tap	**35–110 mill.**

2) Indirekte økonomiske tap

Komponent	Lav	Høy
Privat: tapt tid (7 døgn)	~73 mill.	~394 mill.
Næring: tapt tid (7 døgn)	~84 mill.	~525 mill.
Tjenestefriksjon (betaling/autentisering/ordre)	20 mill.	200 mill.
Sum indirekte tap	**≈ 180 mill.**	**≈ 1 120 mill.**

53 Verdi av tid er basert på dokumentasjonsgrunnlaget til Verdsettingsstudien 2020. Antall 5G-brukere bør korrigeres med operatørdata. Omfanget av brukere som er rammet er veiledende.

3) Total – digital infrastruktur

Type tap	Intervall
Direkte	35–110 mill.
Indirekte	180–1 120 mill.
Total (7 døgn)	**215 mill. – 1,23 mrd. kr**

Finans

Forutsetninger[54]

Parameter	Lav	Høy	Kommentar
Geografisk omfang	Norge, finansmarked + bankoppgjør	Norge + sterk markedsuro	nasjonal systemeffekt
Varighet	7 døgn	7 døgn	av-og-på tidsforstyrrelser
Teknisk effekt	Periodisk usynkronisert tid i utvalgte systemer	Gjentatte sync-feil på tvers av aktører	hovedrisiko: intern tidsuenighet
NBO-omsetning (referanse)	350 mrd/døgn	350 mrd/døgn	gitt i grunnlaget
NBO-oppdrag (referanse)	4 600/døgn	4 600/døgn	gitt i grunnlaget
Berørte bankmiljøer (handel/ oppgjør)	få, avgrenset	flere store aktører	heterogen tidsinfrastruktur
Påvirkning handel (MiFID II-kritisk)	midlertidig nedskalering	periodiske handelsstopp/ avvisning	mikrosekundkrav
Påvirkning massebetaling/kort	liten	moderat	ikke like tidskritisk iht. kap 6

1) Direkte økonomiske tap

Kostnadskomponent	Enhet	Lav	Høy	Sum
Incident response, 24/7 drift, forsterket SOC/NOC	fast (7 døgn)	25 mill.	80 mill.	25–80 mill.
Re-synkronisering/forensikk/validering av tidsstempler og logger	fast	20 mill.	90 mill.	20–90 mill.
Midlertidig omlegging av handels-/oppgjørsflyt	fast	15 mill.	70 mill.	15–70 mill.
Ekstern bistand (teknisk/juridisk/compliance)	fast	10 mill.	40 mill.	10–40 mill.
Mulige tilsyns-/regelverkskostnader (MiFID II-avvik)	fast	0 mill.	150 mill.	0–150 mill.
Sum direkte tap				**70–430 mill.**

54 Kilder for volum, Norges Bank årsrapport

2) Indirekte økonomiske tap

2a) Markedsaktivitet og handel – tapt verdiskaping (konkret mekanisme)

Mekanisme: periodisk manglende tidssynk → redusert/utsatt handel, avviste transaksjoner, lavere markedsdybde, høyere spread og dårligere prisoppnåelse.

Komponent	Lav	Høy
Tapt verdiskaping i marked/handel (7 døgn)	200 mill.	1 600 mill.

2b) Oppgjørsfriksjon og likviditetsbinding

Mekanisme: forsinket matching/oppgjør i tidsvinduer gir midlertidig binding av likviditet, ekstra finansieringskostnader og operativ venting.

Komponent	Lav	Høy
Likviditets- og oppgjørsfriksjon (7 døgn)	120 mill.	900 mill.

2c) Næringsliv/friksjon i betaling og banktjenester

Mekanisme: ikke total svikt i kort/massebetaling, men økt treghet/feilrater i enkelte prosesser, mer manuell håndtering, forsinkede bedriftsbetalinger.

Komponent	Lav	Høy
Betalings- og driftsfriksjon i realøkonomien (7 døgn)	80 mill.	500 mill.

2d) Omdømme- og kundeadferdseffekt

Mekanisme: høyere kundefrafall i enkelte segmenter, lavere aktivitet i berørte tjenester i analyseperioden.

Komponent	Lav	Høy
Kortsiktig omdømme/forretningsfriksjon (7 døgn)	20 mill.	300 mill.

Sum indirekte tap

Komponent	Sum
Marked/handel	200–1 600 mill.
Oppgjør/likviditet	120–900 mill.
Betalings- og driftsfriksjon	80–500 mill.
Omdømme/kundeadferd	20–300 mill.
Sum indirekte tap	**420–3 300 mill.**

3) Samlet økonomisk konsekvens – finans

Type tap	Intervall
Direkte tap	70–430 mill.
Indirekte tap	420–3 300 mill.
Total (7 døgn)	**490 mill. – 3,73 mrd. kr**

Vedlegg 4: Aktører som har vært kontaktet i analysen

Direktoratet for romvirksomhet
Nasjonal sikkerhetsmyndighet

Norges Bank
DNB

Nasjonal kommunikasjonsmyndighet
Telenor
To datasentre

Statnett
Lede

Statens vegvesen

Bane NOR
Jernbanedirektoratet

Avinor
Luftfartstilsynet

DSB

Direktoratet for samfunnssikkerhet og beredskap
Rambergveien 9
3115 Tønsberg

+47 33 41 25 00
postmottak@dsb.no