



FOLKETINGET
STATSREVISORERNE



FOLKETINGET
RIGSREVISIONEN

December 2024
– 7/2024

Rigsrevisionens beretning afgivet
til Folketinget med Statsrevisorernes
bemærkninger

It-sikkerheden i Banedanmarks signalsystem

7/2024

Beretning om

it-sikkerheden i Banedanmarks signalsystem

Statsrevisorerne fremsender denne beretning med deres bemærkninger til Folketinget og vedkommende minister, jf. § 3 i lov om statsrevisorerne og § 18, stk. 1, i lov om revisionen af statens regnskaber m.m.

København 2024

Denne beretning til Folketinget skal behandles ifølge lov om revisionen af statens regnskaber, § 18:

Statsrevisorerne fremsender med deres bemærkning Rigsrevisionens beretning til Folketinget og vedkommende minister.

Transportministeren afgiver en redegørelse til beretningen.

Rigsrevisor afgiver et notat med bemærkninger til ministerens redegørelse.

På baggrund af ministerens redegørelse og rigsrevisors notat tager Statsrevisorerne endelig stilling til beretningen, hvilket forventes at ske i april 2025.

Ministerens redegørelse, rigsrevisors bemærkninger og Statsrevisorernes eventuelle bemærkninger samles i Statsrevisorernes Endelig betænkning over statsregnskabet, som årligt afgives til Folketinget i februar måned – i dette tilfælde Endelig betænkning over statsregnskabet 2024, som afgives i februar 2026.

Statsrevisorernes bemærkning tager udgangspunkt i denne karakterskala:

Karakterskala

Positiv kritik	<ul style="list-style-type: none">• finder det meget/særdeles positivt• finder det positivt• finder det tilfredsstillende/er tilfredse med
Kritik under middel	<ul style="list-style-type: none">• finder det ikke helt tilfredsstillende
Middel kritik	<ul style="list-style-type: none">• finder det utilfredsstillende/er utilfredse med• påpeger/understreger/henstiller/forventer• beklager/finder det bekymrende/foruroligende
Skarp kritik	<ul style="list-style-type: none">• kritiserer/finder det kritisabelt/kritiserer skarpt/indskærper• påtaler/påtaler skarpt
Skarpeste kritik	<ul style="list-style-type: none">• påtaler skarpt og henleder særligt Folketingets opmærksomhed på

**Henvendelse vedrørende
denne publikation rettes til:**

Statsrevisorerne
Folketinget
Christiansborg
1240 København K

Tlf.: 3337 5987
statsrevisorerne@ft.dk
www.ft.dk/statsrevisorerne

ISSN: 2245-3008
ISBN online 978-87-7434-851-1

Statsrevisorernes bemærkning

Beretning om it-sikkerheden i Banedanmarks signalsystem

Banedanmark har ansvaret for at drive, vedligeholde og udvikle den stats-ejede jernbaneinfrastruktur. Frem mod 2033 udskifter Banedanmark alle analoge signaler langs jernbanen med et digitalt signalsystem. Signalsystemet styrer trafikken på jernbanen.

Signalsystemet er et af statens ca. 90 samfundskritiske it-systemer, dvs. et system, hvor større driftsforstyrrelser resulterer i væsentlige udfordringer for samfundet. Center for Cybersikkerhed vurderer, at risikoen for cyberkriminalitet mod jernbanesektoren er meget høj.

Undersøgelsen har til formål at vurdere, om Banedanmark har sikret en tilfredsstillende it-sikkerhed i signalsystemet, der kan modstå hændelser, som kan medføre nedbrud i signalsystemet. Undersøgelsens resultater er omgivet af fortrolighed, fordi oplysninger herom kan eksponere sårbarheder i signalsystemet og dermed øge trusselsniveauet mod Banedanmark.

Statsrevisorerne finder det kritisabelt, at Banedanmark har væsentlige sårbarheder i it-sikkerheden i signalsystemet. Det indebærer en risiko for, at sikkerhedshændelser kan forstyrre og standse togdriften, hvilket vil være til stor gene for brugerne. Længerevarende nedbrud kan dertil have betydning for samfundsøkonomien.

Statsrevisorerne påtaler, at Banedanmarks it-sikkerhed ikke opfylder 10 af de 19 undersøgte vurderingskriterier. 6 af vurderingskriterierne er delvist opfyldt. Bl.a. vurderer Rigsrevisionen, at de handlingsplaner, som Banedanmark allerede har udarbejdet, ikke er fyldestgørende. 3 af vurderingskriterierne er opfyldt.

Statsrevisorerne finder det særdeles nødvendigt, at Banedanmark hurtigst muligt får rettet op på de mangler i it-sikkerheden, som undersøgelsen har påvist.

Statsrevisorerne

9. december 2024

Serdal Benli
Leif Lahn Jensen
Mikkel Irminger Sarbo
Lars Christian Lilleholt
Monika Rubin
Mai Mercado

Indholdsfortegnelse

1. Indledning.....	1
1.1. Formål og konklusion.....	1
1.2. Baggrund.....	4
1.3. Vurderingskriterier, metode og afgrænsning.....	7
2. It-sikkerheden i signalsystemet.....	8
Bilag 1. Metodisk tilgang.....	10

Rigsrevisionen har selv taget initiativ til denne undersøgelse og afgiver derfor beretningen til Statsrevisorerne i henhold til § 17, stk. 2, i rigsrevisorloven, jf. lovbekendtgørelse nr. 101 af 19. januar 2012.

Rigsrevisionens mandat til at gennemføre undersøgelsen følger af § 2, stk. 1, nr. 1, jf. § 3 i rigsrevisorloven.

Beretningen vedrører finanslovens § 28. Transportministeriet.

I undersøgelsesperioden januar-marts 2024 har der været følgende ministre:

Thomas Danielsen: december 2022 -

Beretningen har i udkast været forelagt Transportministeriet, herunder Banedanmark, hvis bemærkninger i videst muligt omfang er afspejlet i beretningen.

1. Indledning

1.1. Formål og konklusion

1. Denne beretning handler om it-sikkerheden i Banedanmarks signalsystem. Signalsystemet sender signaler mellem tog og trafikstyringscentraler og styrer derigennem trafikken på jernbanen.

2. Jernbanen er en væsentlig del af den offentlige infrastruktur. Jernbanen består af mere end 3.000 km spor og omfatter også en række kritiske dele, som understøtter togdriften, fx radiomaster, fiberkabler, strømnet og signalsystemet. Jernbanen er derfor sårbar over for hændelser af forskellig karakter, og Banedanmark står således over for en bred vifte af mulige hændelser, der kan påvirke den fysiske og digitale infrastruktur og derved forstyrre togdriften. Banedanmark skal som ansvarlig myndighed prioritere indsatsen i forhold til de forskellige risici, som jernbanen står over for.

Center for Cybersikkerhed vurderer, at risikoen for cyberkriminalitet mod jernbanesektoren er meget høj, og at jernbanesektorens it-leverandører er oplagte mål for hackerangreb. At risikoen er reel, kunne man se et eksempel på i november 2022. DSB blev via en app hos en leverandør udsat for et hackerangreb, som stoppede S-togstrafikken i flere timer.

3. Banedanmark har igangsat en modernisering af jernbanens signalsystem med et samlet budget på ca. 22 mia. kr. (2024-priser). Frem mod 2033 udskifter Banedanmark alle analoge signaler langs jernbanen med et digitalt signalsystem. Signalsystemet skal oplyse lokomotivføreren om, hvorvidt toget skal køre eller holde stille, og dermed bl.a. sikre, at togene ikke støder sammen. Da signalsystemet er digitalt, medfølger en række risici vedrørende it-sikkerhed. Banedanmark definerer signalsystemet som et samfundskritisk it-system, dvs. et system, hvor større driftsforstyrrelser resulterer i væsentlige udfordringer for samfundet. Nedbrud i signalsystemet vil have konsekvenser for både passagerer og godstransport, og længerevarende nedbrud kan have samfundsøkonomiske konsekvenser.

4. Formålet med undersøgelsen er at vurdere, om Banedanmark har sikret en tilfredsstillende it-sikkerhed i signalsystemet til at kunne modstå hændelser, der kan medføre nedbrud i signalsystemet.

Rigsrevisionen har selv taget initiativ til undersøgelsen i november 2023.

Signalsystemet

Signalsystemet omfatter fjernbanen og S-togsbanen. Denne undersøgelse omhandler kun signalsystemet på fjernbanen.

Fjernbanen er en betegnelse for det landsdækkende toget, der primært omfatter fjern- og regionaltog. Fjernbanen betjener store dele af landet og forbinder de større byer. Banedanmark står for at vedligeholde infrastrukturen, mens DSB og Arriva varetager togdriften.

5. Undersøgelsen tager udgangspunkt i den internationale standard for informations-sikkerhed ISO 27001. Det har siden 2016 været obligatorisk for statslige myndigheder at følge standarden.

Udgangspunktet for ISO 27001 er, at den enkelte myndighed skal vurdere de risici på it-området, som myndigheden står over for. Risikovurderingen hjælper myndigheden med at kortlægge, hvor det er vigtigst at højne it-sikkerheden. På baggrund af risikovurderingen prioriterer myndigheden i en handlingsplan de foranstaltninger, som myndigheden vurderer er mest hensigtsmæssige. Myndigheden kan som led i prioriteringen vælge at acceptere visse risici og i stedet gennemføre foranstaltninger på andre områder.

Vi har taget udgangspunkt i 19 vurderingskriterier, som følger af ISO 27001, men som er tilpasset de specifikke rammer, der gælder for Banedanmark. Vi har i løbet af undersøgelsen tilpasset kriterierne for at sikre, at vi har undersøgt de vigtigste og mest kritiske dele af it-sikkerheden i signalsystemet. Det er vores vurdering, at vi på baggrund af de 19 kriterier kan foretage en samlet vurdering af it-sikkerheden i signalsystemet.

Vi har brugt samme metode i flere lignende undersøgelser. Vi har bl.a. undersøgt it-sikkerheden hos statslige myndigheder i beretningen om Energinets outsourcing af driften af forsyningskritisk infrastruktur (nr. 14/2021) og beretningerne om statens it-beredskab (nr. 3/2022 og nr. 5/2023).

6. Banedanmark har vurderet, at de problemer med it-sikkerheden, som Rigsrevisionens undersøgelse har afdækket, er fortrolige oplysninger, da de kan eksponere sårbarheder i signalsystemet og dermed øge trusselsniveauet mod Banedanmark. Banedanmark har oplyst, at problemerne kun kan have konsekvenser for længden og omfanget af driftsafbrydelser, og at problemerne ikke har betydning for passagerernes sikkerhed eller sikkerheden i den generelle drift.

Rigsrevisionen har imødekommet Banedanmarks ønske om fortrolighed. Beretningen indeholder derfor kun overordnede og summariske beskrivelser af problemerne med it-sikkerheden i signalsystemet.

Rigsrevisionens seneste beretninger om it-sikkerheden i staten

- Beretning om Energinets outsourcing af driften af forsyningskritisk infrastruktur (nr. 14/2021)
- Beretning om statens it-beredskab (nr. 3/2022)
- Beretning om statens it-beredskab II (nr. 5/2023)
- Beretning om it-sikkerheden på Statens It's servere (nr. 6/2023)
- Beretning om Finanstilsynets it-tilsyn (nr. 14/2023).



Konklusion

Banedanmark har væsentlige sårbarheder i it-sikkerheden i signalsystemet. Dette finder Rigsrevisionen meget utilfredsstillende. Konsekvensen er, at der er risiko for, at it-sikkerhedshændelser kan forstyrre eller standse togdriften, hvilket vil være til stor gene for passagerer og virksomheder. Længerevarende nedbrud kan også have betydning for samfundsøkonomien.

1.2. Baggrund

Digitalisering af jernbanen

7. Banedanmark er som styrelse under Transportministeriet ansvarlig for at drive jernbanen. Banedanmark igangsatte i 2009 et projekt – Signalprogrammet – der har til formål at modernisere jernbanen. Formålet er ifølge Banedanmark at udskifte de nuværende analoge signaler, som ofte fører til fejl og forsinkelser, med digitale løsninger. Det gamle signalsystem er primært baseret på anlæg fra 1950'erne og 1960'erne. De ældste anlæg blev dog udviklet i 1912.



Ældre sikringsanlæg på Struer Station. Anlægget er taget ud af drift i februar 2021.

Foto: Banedanmark

8. Signalsystemet er et teknologisk løft, der skal forbedre sikkerheden på jernbanen og sikre, at togene kan køre hurtigere og i højere grad til tiden. Banedanmark bruger flere eksterne leverandører til it-driften af signalsystemet. Selv om it-driften er outsourcet, er det fortsat Banedanmarks ansvar at sikre den fornødne it-sikkerhed.

Udrulningen af signalsystemet er blevet forsinket flere gange. Senest er det udrulningen af signalsystemet på strækninger på Fyn og Sjælland, der har været udfordret. Det drejer sig bl.a. om strækningerne København-Helsingør og København-Roskilde. Forsinkelserne betyder, at Banedanmark nu forventer, at udrulningen er afsluttet i 2033. Det er 12 år senere end oprindeligt planlagt.

De første strækninger med signalsystemet blev taget i brug i 2018 og er løbende blevet udbygget, så systemet i dag er taget i brug på ca. halvdelen af de planlagte strækninger. Vest for Lillebælt er 5 ud af 9 strækninger taget i brug, hvilket svarer til mere end 600 km jernbane. Øst for Lillebælt er 4 ud af 10 strækninger taget i brug, hvilket svarer til mere end 160 km jernbane.

Figur 1 viser de strækninger, som er taget i brug (ubrudt grøn linje), og de strækninger, som skal bruge signalsystemet, men som endnu ikke har taget systemet i brug (stiplet grøn linje).

Figur 1
Status på udrulningen af signalsystemet (2024)



Kilde: Rigsrevisionen på baggrund af oplysninger fra Banedanmark.

Signalsystemets opbygning

9. I beretningen bruger vi betegnelsen *signalsystemet* som en samlet betegnelse for flere it-systemer, der tilsammen erstatter de analoge signaler langs jernbanen. Togene styres centralt af 2 trafikstyringscentraler. Den ene er placeret i Fredericia til at styre trafikken i Vestdanmark, og den anden er placeret i København til at styre trafikken i Østdanmark. I hvert tog er der installeret et it-system, som digitalt modtager signaler fra den relevante trafikstyringscentral.

1.3. Vurderingskriterier, metode og afgrænsning

Vurderingskriterier

10. Vores undersøgelse er baseret på 19 vurderingskriterier, som følger af sikkerhedsstandarden ISO 27001, og som er væsentlige for at give en samlet vurdering af it-sikkerheden i signalsystemet.

Banedanmark har udarbejdet egne retningslinjer og sikkerhedspolitikker for signalsystemet, der ligesom vores vurderingskriterier følger af ISO 27001. Vi vurderer dermed i et vidt omfang, om Banedanmark i praksis efterlever sine egne retningslinjer og sikkerhedspolitikker.

Metode

11. Undersøgelsen baserer sig på dokumentgennemgang. Vi har desuden kontrolleret udvalgt materiale fra Banedanmark ved hjælp af data fra signalsystemet.

12. Undersøgelsens metode uddybes i bilag 1.

13. Revisionen er udført i overensstemmelse med standarderne for offentlig revision, jf. bilag 1.

Afgrænsning

14. Undersøgelsen omfatter kun it-sikkerheden for de dele af Banedanmarks signalsystem, som er taget i brug på fjernbanen. Undersøgelsen omfatter dermed ikke strækninger, der endnu ikke er taget i brug, og heller ikke it-sikkerheden for S-togsnettet.

15. Undersøgelsen er afgrænset fra at undersøge den fysiske sikkerhed vedrørende jernbanen, fx sikring af togskiner.

16. Undersøgelsen af signalsystemets it-sikkerhed er gennemført i perioden januar-marts 2024. Undersøgelsen omhandler dermed det sikkerhedsbillede, der var aktuelt på dette tidspunkt, og omfatter ikke eventuelle initiativer, som Banedanmark efterfølgende har gennemført.

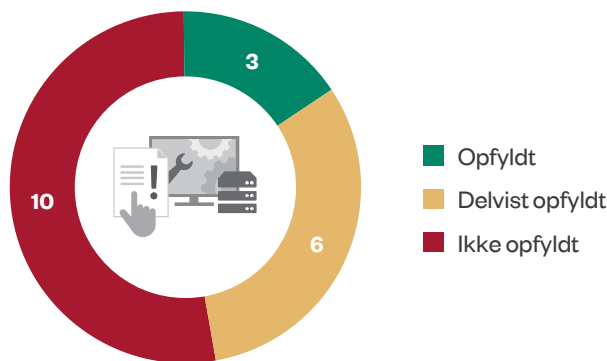
2. It-sikkerheden i signalsystemet

17. Dette kapitel handler om, hvorvidt Banedanmark har sikret en tilfredsstillende it-sikkerhed i signalsystemet. For at vurdere dette har vi undersøgt it-sikkerheden i signalsystemet med udgangspunkt i 19 vurderingskriterier.

Undersøgelsen viser, at Banedanmark samlet set ikke har sikret en tilfredsstillende it-sikkerhed i signalsystemet.

18. Figur 2 viser det samlede resultat af vores undersøgelse af de 19 vurderingskriterier.

Figur 2
It-sikkerheden i signalsystemet fordelt på 19 vurderingskriterier



Kilde: Rigsrevisionen på baggrund af oplysninger fra Banedanmark.

Det fremgår af figur 2, at signalsystemet ikke lever op til 10 af de 19 vurderingskriterier. Det fremgår desuden, at 6 kriterier er delvist opfyldt, og at 3 kriterier er opfyldt.

19. De fleste resultater af undersøgelsen kan ikke offentliggøres, da Banedanmark har vurderet, at der er tale om fortrolige oplysninger, som kan eksponere sårbarheder i signalsystemet. Det samme gælder de vurderingskriterier, vi har brugt i undersøgelsen, og de aktiviteter, vi har gennemført.

Boks 1 og boks 2 viser eksempler på resultater, som Banedanmark vurderer ikke kan udnyttes til at kompromittere it-sikkerheden. Banedanmark har som en del af undersøgelsen modtaget en udførlig gennemgang af alle resultaterne.

Boks 1**Eksempel 1**

Det fremgår af ISO 27001, at it-systemer skal risikovurderes. Risikovurderingerne skal beskrive potentielle trusler mod systemerne, fx cyberangreb, risiko for nedbrud og andet, der kan påvirke driften af systemerne. Risikovurderingerne skal også beskrive, hvordan risiciene skal håndteres. Det fremgår desuden af ISO 27001, at der på baggrund af risikovurderingerne skal udarbejdes handlingsplaner, som adresserer de identificerede risici.

Rigsrevisionens undersøgelse viser, at Banedanmark har foretaget risikovurderinger af signalsystemet. Undersøgelsen viser dog, at Banedanmark ikke har udarbejdet relevante handlingsplaner på baggrund af risikovurderingerne. Der er dermed ikke relevante handlingsplaner for, hvordan Banedanmark vil håndtere de risici, der er identificeret i risikovurderingerne.

Banedanmark har oplyst, at der for en del af risikovurderingerne er udarbejdet handlingsplaner. Banedanmark vil sikre, at der udarbejdes handlingsplaner for de resterende risikovurderinger. Rigsrevisionen vurderer, at de handlingsplaner, som Banedanmark allerede har udarbejdet, ikke er fyldestgørende.

Boks 2**Eksempel 2**

Det fremgår af ISO 27001, at udvikling og test af funktioner i it-systemer skal ske i et testmiljø og dermed være adskilt fra driftsmiljøet. Dette fremgår også af Banedanmarks egne retningslinjer. Det er vigtigt, at udvikling og test er adskilt fra driftsmiljøet, fordi udvikling og test ikke skal kunne påvirke driften af systemet.

Rigsrevisionens undersøgelse viser, at der på bestemte områder udføres tests i selve signalsystemet. Der er risiko for, at disse tests kan påvirke driften af signalsystemet og dermed togdriften.

Banedanmark har oplyst, at der allerede er igangsat flere initiativer til at adskille testmiljøet fra driftsmiljøet. Banedanmark forventer bl.a. at gennemføre analyser af de omkostninger, der er forbundet med at gennemføre tests uden for selve signalsystemet.

20. Rigsrevisionen vil som led i opfølgningen på denne beretning følge Banedanmarks arbejde med at sikre en tilfredsstillende it-sikkerhed i Banedanmarks signalsystem.

Rigsrevisionen, den 28. november 2024

Birgitte Hansen

/Mads Nyholm Jacobsen

Bilag 1. Metodisk tilgang

Undersøgelsen bygger på en gennemgang af dokumenter og møder med relevante medarbejdere fra Banedanmark og Transportministeriets departement. Undersøgelsen er desuden på udvalgte områder kvalitetssikret ved demonstrationer, oversigter og skærbilleder for at efterprøve den information, vi har fået.

Undersøgelsens vurderingskriterier baserer sig på den internationale standard for informationssikkerhed ISO 27001. Vi har tilpasset kriterierne ud fra en konkret vurdering af, hvilke kriterier der er de mest centrale for undersøgelsen. Det har vi gjort for at sikre, at vi har undersøgt de vigtigste og mest kritiske områder af signalsystemet.

Beretningen omfatter perioden januar-marts 2024.

Væsentlige dokumenter

Vi har gennemgået en række dokumenter, herunder:

- Banedanmarks risikovurderinger, handlingsplaner og dispensationer for signalsystemet
- Banedanmarks politik og organisering af informationssikkerhed og risikostyring
- Banedanmarks fortegnelse over samfundskritiske processer, systemer og infrastruktur
- Banedanmarks kontrakter med leverandørerne af signalsystemet
- referater af udvalgte møder mellem Banedanmark og leverandørerne af signalsystemet
- Banedanmarks beredskabs- og indsatsplaner samt testplaner for samme
- Banedanmarks politik for adgangsstyring, brugernavne og passwords
- Banedanmarks politik for driftssikkerhed
- oversigt over servere, der understøtter signalsystemet
- oversigt over netværksenheder, der understøtter signalsystemet
- oversigt over systemlandskabet for signalsystemet
- Banedanmarks vejledning for logning
- Banedanmarks procedurer for ændrings- og fejlhåndtering.

Vi har desuden gennemgået systemdokumentationen for udvalgte gennemførte ændringer i signalsystemet for at vurdere processen for ændringsstyring.

Møder

Vi har holdt møder med Banedanmark og Transportministeriets departement for at få indsigt i området og for at få gennemgået og uddybet det materiale, vi har modtaget i forbindelse med gennemgangen af hvert vurderingskriterie. Vi har især holdt en række møder med relevante medarbejdere fra Banedanmark, som arbejder inden for de områder, som vurderingskriterierne dækker over.

Møderne har været struktureret ud fra følgende:

- gennemgang af vurderingskriteriet
- gennemgang af Banedanmarks politikker og retningslinjer inden for vurderingskriteriets område
- gennemgang af dokumentation og Banedanmarks redegørelse for opfyldelse af vurderingskriteriet.

Kvalitetssikring

Undersøgelsen er kvalitetssikret via vores interne procedurer for kvalitetssikring, som omfatter høring hos den reviderede samt ledelsesbehandling og sparring med chefer og medarbejdere i Rigsrevisionen.

Standarderne for offentlig revision

Revisionen er udført i overensstemmelse med standarderne for offentlig revision, herunder standarderne for større undersøgelser (SOR 3). Standarderne fastlægger, hvad brugerne og offentligheden kan forvente af revisionen, for at der er tale om en god faglig ydelse. Standarderne er baseret på de grundlæggende revisionsprincipper i rigsrevisionernes internationale standarder (ISSAI 100-999).