Statens Havarikommisjon for Transport

JB Rapport: 2007/02

RAPPORT OM ALVORLIGE JERNBANEHENDELSER PÅ SLEPENDEN BLOKKPOST PÅ GRUNN AV SIGNALFEIL VED SANDVIKA STASJON 20. APRIL 2005

Avgitt
Februar 2007

Statens Havarikommisjon for Transport
Postboks 213
2001 Lillestrøm
Telefon: 63 89 63 00
Faks: 63 89 63 01
http://www.aibn.no
E-post: post@aibn.no

INNHOLDSFORTEGNELSE

RAPPORT OM

Sikringsanlegg:	Stillverk, Siemens type SIMIS-C
Tognummer:	13905 og 12207
Involvert materiell:	Type 71 og Type 69
Registrering:	Flytog 71005 og NSB tog 69072
Eiere:	Flytoget AS og NSB AS
Brukere:	Flytoget AS og NSB AS
Besetning:	En flytogfører/lokomotivfører var om bord i hvert tog.
Passasjerer:	Ingen, (begge de involverte tog var tomtog)
Hendelsessted:	Sandvika stasjon - Slependen blokkpost
Hendelsestidspunkt:	Hendelse 1, onsdag 20. april 2005 kl. 0418 Hendelse 2, onsdag 20. april 2005 kl. 0444

MELDING OM HAVARIET

Havarikommisjonen ble umiddelbart varslet om de alvorlige hendelsene av vakthavende personale fra Flytoget AS og Jernbaneverket. Innrapportering fra NSB AS ble foretatt senere samme dag. Dette skyldes at den alvorlige hendelsen ikke umiddelbart ble innrapportert til Driftsoperativt senter for NSB AS.

SAMMENDRAG

Onsdag 20. april 2005, i tidsrommet kl. 0418 – 0444, skjedde det to alvorlige hendelser i forbindelse med at et forsignal hadde vist feil signalbilde. Hendelse 1 inntraff kl. 0418 da flytog 13905 hadde passert forsignal A for Slependen, som viste signal ”vent kjør”, og nærmet seg blokksignal A 357 på Slependen blokkpost. Da oppdaget flytogføreren at blokksignalet viste signal ”stopp”. Flytogføreren foretok umiddelbart nødbrems på toget, men da det kun var en kort strekning fram til blokksignalet klarte han ikke å stoppe foran signalet, men passerte signalet med hele toget. Det befant seg da to tog på samme blokkstrekning. Hendelse 2 inntraff kl. 0444 da neste tog, 12207 passerte forsignalet for Slependen blokkpost og dette viste signal ”vent kjør”. Togets ATC-utrustning viste kjør i

hovedindikatoren, og toget fortsatte ut på blokkstrekningen i en hastighet på nærmere 82 km/h. Da toget nærmet seg Slependen holdeplass oppdaget lokomotivføreren 2 røde lys (baklysene på flytog 13905) i et av sporene og foretok umiddelbart nødbrems. Han fikk stoppet toget få meter fra flytoget, som noen minutter tidligere hadde stoppet i samme spor. Avstanden fram til flytog 13905 var da omtrent 30 meter. Det var kun lokomotivførerens årvåkenhet og snarrådige handling som forhindret at dette ble et sammenstøt.

Ved gjennomgang av sikringsanlegget viste det seg at det var en programfeil i datastillverket. Denne programfeilen ble identifisert i den generiske programvaren. For at denne feilen skulle kunne oppstå, var det 4 forhold som måtte inntreffe i en bestemt rekkefølge. Dette trigget stillverket slik at forsignalet viste feil (ikke restriktivt) signalbilde. Alle sikringsanlegg med tilsvarende grensesnitt ble satt ut av drift inntil systemfeilen i datastillverket hadde blitt rettet, testet og driftsprøvd.

ENGLISH SUMMARY

Wednesday 20 April two serious incidents happened at Slependen block station as a result of a distant signal displaying an incorrect signal light. At the first incident an airport express train passed the distant signal displaying one green light. This told the driver that the next block signal was green. However, when the train approached the block signal this proved to be red. The locomotive driver immediately activated emergency braking but could not prevent that the whole train passed the block signal before stopping. As there already was a train further ahead on this block section, there were now two trains on the same section.

The second serious incident happened some minutes later when a passenger train passed the same distant signal. Similar to the first incident, the distant signal light was green even though at this moment in time there were two trains on the next block section. The train's ATC system confirmed that the next block signal was indeed green and the train approached the signal at a speed of 82 km/h. As the train came nearer to the block signal, the locomotive driver caught sight of two red lights on the line ahead. He immediately activated emergency braking and thus managed to stop the train approximately 30m behind the train ahead. The vigilance and resourcefulness of the driver in this situation prevented a certain collision.

The investigation of the signal system identified a programming error in the generic software of the system. In addition, four different and unrelated failure states were present in the signal system when the distant signal displayed the wrong light.

For this signal failure to happen, the investigation proved that the four failure states had to occur in a specific sequence in combination with the generic software error.

All signal systems with the same interface were disabled until the software system failure had been identified, repaired and controlled.

1. FAKTISKE OPPLYSNINGER

1.1 Hendelsesforløpet

Onsdag 20. april 2005 i tidsrommet kl. 0418 – 0444 skjedde det to alvorlige hendelser i forbindelse med at et forsignal hadde vist feil signalbilde. Det aktuelle forsignalet var plassert på samme mast som utkjørhovedsignal N 4323 på Sandvika stasjon, og var et signal som forvarslet hva blokksignal A 357 på Slependen blokkpost i retning Asker viste. Blokksignal A 357 på Slependen blokkpost viste ”signal stopp, (rødt lys) samtidig som forsignalet på signal N 4323 viste signal vent kjør (se fig. 1 og 2). Forriglingen i stillverket skal være konstruert slik at det ikke skal være mulig for denne kombinasjonen å inntreffe.

Oversikt over hendelsesforløpet i tid.

- Arbeidstog 51006 disponerer linjen mellom Billingstad og Hvalstad for arbeider fram til kl. 0500.

- Kl 0400. Tog 13903 passerer signal B Slependen blokkpost, blir stående foran innkjørhovedsignal A på Billingstad for å vente på at motgående tog 3701 skal passere på hovedspor Drammen – Oslo.

- Kl 0417. Tog 13905 passerer utkjørhovedsignal N (4323) på Sandvika stasjon.

- Kl. 0419. Tog 13905 passerer signal A Slependen (passerer med hele togsettet og linjeblokka blir fri bak togsettet). Flytogføreren melder fra til togleder om signalfeilen. To tog befinner seg nå på samme blokkstrekning

- Kl 0422. Tog 13903 får ”signal kjør” inn på Billingstad stasjon

- Kl 0438. Tog 12207 kjører inn i spor 1 på Sandvika stasjon.

- Kl 0441. Stilles innkjørhovedsignal på Billingstad til ”signal kjør” for tog 13905, men toget blir stående da flytogføreren ikke ser signalet fra denne posisjonen.

- Kl 0442. Stilles utkjørhovedsignal til ”signal kjør” for tog 12207 ut fra spor 1 på Sandvika stasjon

- Kl 0444. Tog 12207 står på linjeblokka like foran signal A Slependen blokkpost.

- Kl 0454. Tog 13905 kjører inn på Billingstad stasjon (passerer signal A 351)

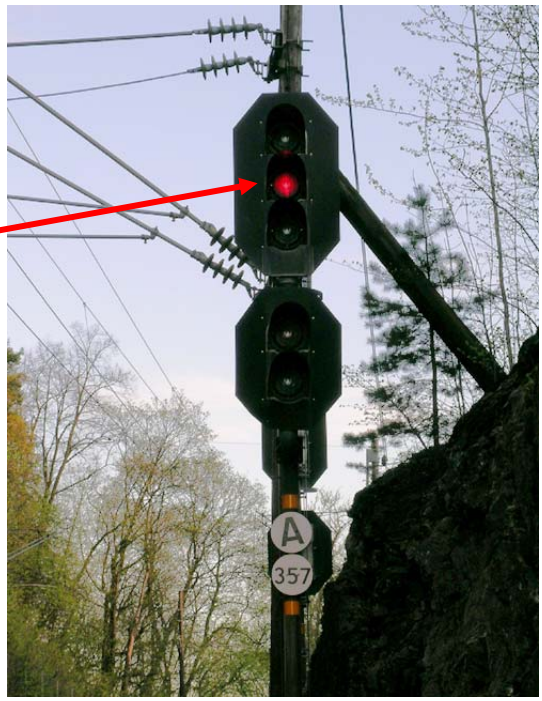
Hendelse 1:

Flytog 13905 hadde passert forsignalet for blokkposten som viste signal ”vent kjør”, og nærmet seg blokksignal A 357 på Slependen blokkpost, da flytogføreren oppdaget at signalet viste signal ”stopp”. Flytogføreren tok umiddelbart nødbrems, men siden det kun var en kort strekning fram til blokksignalet, klarte han ikke å stoppe toget foran signalet.

Toget passerte signalet med hele togsettets lengde og stoppet med togsettets bakre ende noen meter forbi blokksignalet, slik at togets bakenforliggende blokkstrekning ble fri for tog (Se figur 4). Flytogføreren varslet umiddelbart togleder og opplyste at det ikke var samsvar mellom signalbildet i forsignalet og blokksignal A på Slependen blokkpost. Han opplyste også til togleder at togets ATC panel hadde vist tre streker, noe som betyr at Slependen blokkpost skulle vise signal ”kjør”.

Figur 1:

Forsignalet for Slependen blokkpost (plassert på Utkjørhovedsignal N 4323 på Sandvika stasjon), viste signal ”vent kjør”.

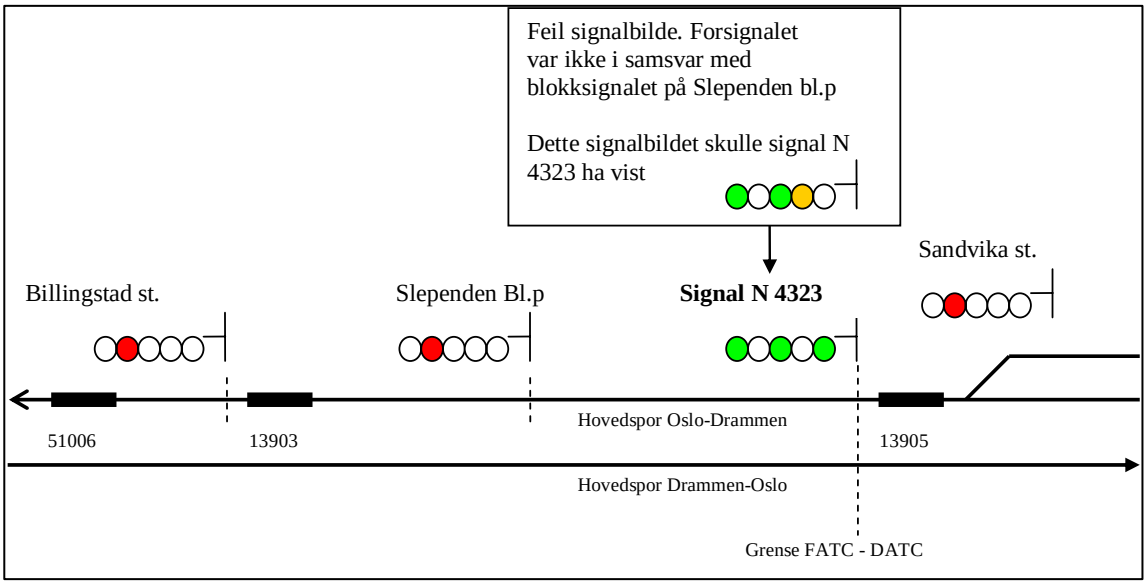


Figur 2:

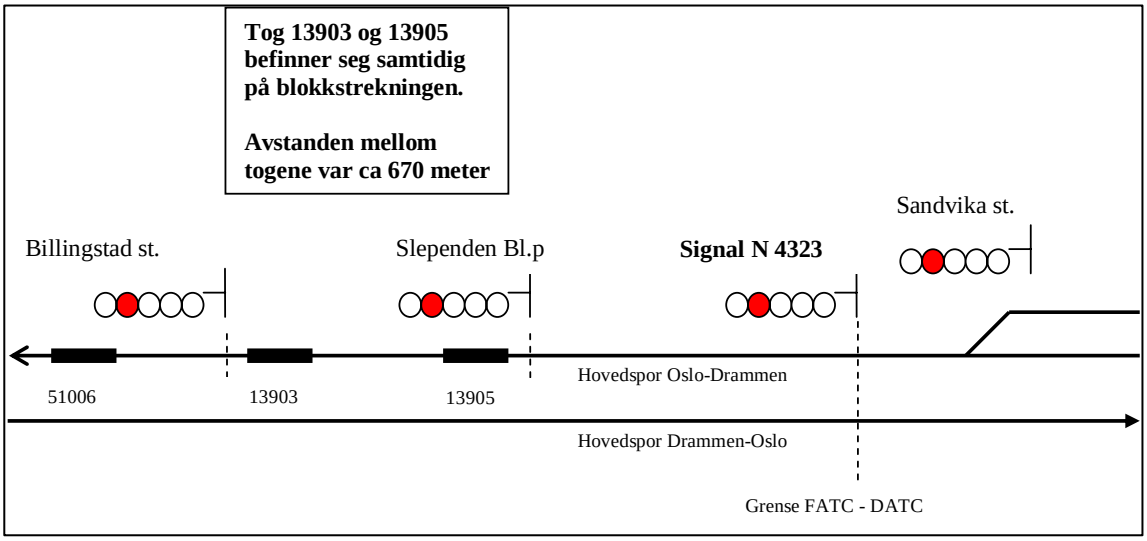
Blokksignal A Slependen viste signal ”stopp”. (Ikke samsvar med signalbildet i forsignalet)

Grunnen til at blokksignal A 357 på Slependen blokkpost viste ”signal stopp” for flytog 13905, var at flytog 13903 hadde fått signal ”stopp” foran innkjørhovedsignal A på Billingstad stasjon og befant seg på blokkstrekningen mellom Slependen blokkpost og Billingstad stasjon (se fig. 3). Flytog 13903 hadde fått signal ”stopp” i innkjørhovedsignalet på Billingstad stasjon fordi arbeidstog 51006 utførte arbeider på sporet mellom stasjonene Billingstad og Hvalstad. Togleder fikk derfor ikke sendt flytog 13903 videre mot Asker stasjon.

Avstanden mellom flytogene 13903 og 13905 som da befant seg på den samme blokkstrekningen, var cirka 670 meter. Det var ved denne hendelsen ikke fare for sammenstøt mellom disse to togene. (se fig. 4)



Figur 3: Flytog 13905 kjører kl. 0417 ut fra Sandvika stasjon



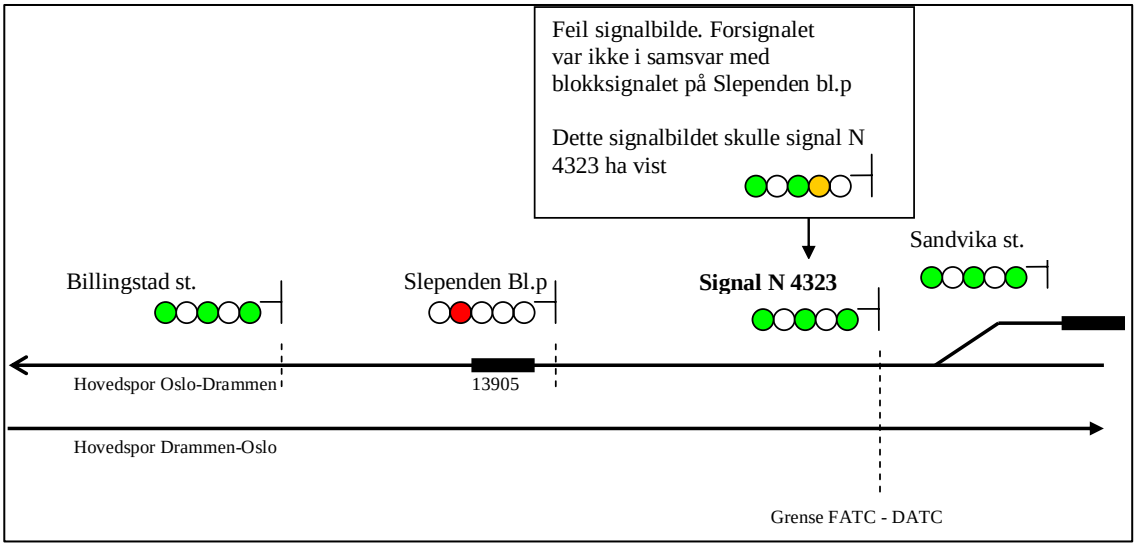
Figur 4: Flytogene 13903 og 13905 befinner seg kl. 0419 på samme blokkstrekning

Flytogføreren i tog 13905 hadde ringt til togleder umiddelbart etter den første alvorlige hendelsen og opplyst at det ikke var samsvar mellom signalbildene i forsignal og blokksignal A 357 i Slependen blokkpost.

Togleder reagerte ikke umiddelbart på denne meldingen, da det ble stilt togvei for tog 12207. I mellomtiden hadde flytogføreren i tog 13905, i samråd med flytogets driftsoperative leder, forflyttet seg til det motsatte førerrommet på togsettet. Han oppdaget da at det hadde stoppet et tog bare få meter fra hans togsett. Flytogføreren ringte på nytt (etter hendelse 2) inn til togleder og informerte om dette.

Hendelse 2:

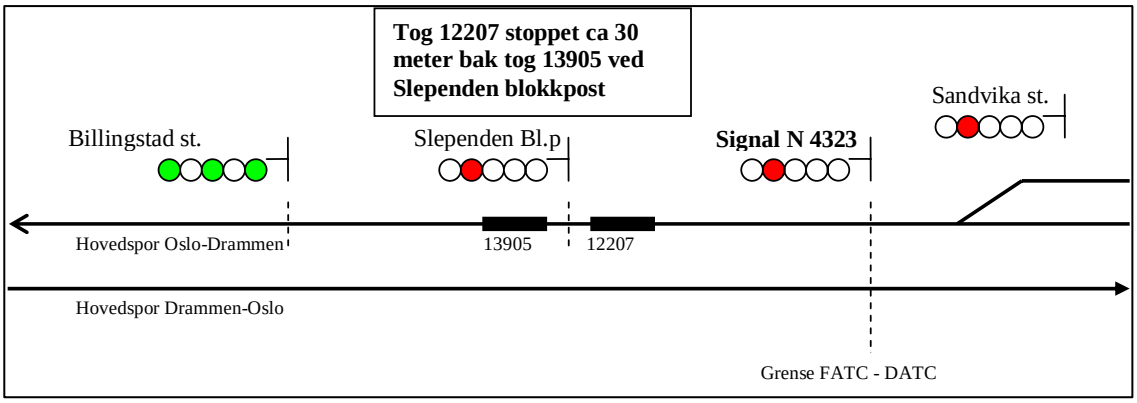
Det var stilt togvei ut fra spor 1 på Sandvika stasjon for tog 12207 ved at utkjørhovedsignal N 4323 viste signal ”kjør” for NSB-tog 12207. Toget passerte utkjørhovedsignalet og forsignalet for Slependen blokkpost viste signal ”vent kjør” (se figur 5). Togets ATC utrustning fikk samme informasjon og toget fortsatte ut på blokkstrekningen i en hastighet på nærmere 82 km/h.



Figur 5: Situasjonen kl. 04:42:46, rett før den andre alvorlige hendelsen inntraff. Tog 12207 startet å kjøre ut fra spor 1 på Sandvika stasjon.

Da toget nærmet seg Slependen holdeplass ble lokomotivføreren i tvil, idet han oppdaget 2 røde lys i et av sporene. Dette var baklysene på tog 13905 som stod på blokkstrekningen etter Slependen blokkpost. Han kunne ikke fastslå hvilket av hovedsporene de røde lysene befant seg i, men tok for sikkerhets skyld umiddelbart nødbrems og oppdaget etter hvert at tog 13905 stod i det samme hovedsporet som han kjørte i. Lokomotivføreren fikk som følge av nødbremsingen stoppet toget like foran signalet på Slependen blokkpost. Vedkommende antok at avstanden fram til flytog 13905 var ca 30 meter. Det var kun lokomotivførerens årvåkenhet og snarrådige reaksjon som forhindret at dette ble et sammenstøt.

Lokomotivføreren hadde hatt nattjeneste og var på slutten av sin arbeidsøkt, og kunne i ettertid ikke erindre hvilket signalbilde som hadde vært i forsignalet, men reagerte på at ikke ATC hadde grepet inn. Det ble ikke umiddelbart meldt fra til togleder om denne alvorlige hendelsen. Dette ble først kjent ca 1,5 time senere, etter at driftsoperativt senter ved NSB hadde tatt kontakt med lokomotivføreren i tog 12207 og deretter varslet togledelsen.



Figur 6: Kl.04:44:31. Situasjonsbilde etter at lokomotivføreren hadde tatt nødbrems og stoppet tog 12207 foran signalet på Slependen blokkpost.

Først etter at de to alvorlige hendelsene hadde blitt innrapportert, ble det hos togledelsen stilt spørsmålstegn ved stillverket på Sandvika stasjon. Vaktleder besluttet at togpersonalet om bord i flytog 13907 skulle iaktta signalbildet i forsignalet og melde fra når toget passerte utkjørhovedsignal N 4323 på Sandvika stasjon. Togpersonalet bekreftet at signal N 4323 virkelig viste det signalbildet som er beskrevet i de to alvorlige hendelsene. På dette tidspunktet ble det satt i verk videre aksjoner fra togledelsen, og feil på sikringsanlegget ble videreformidlet til signalvakta.

Sporets trasé mellom Sandvika og Billingstad ligger i kurvatur. På grunn av at overbygningen på Slependen holdeplass skjermet for sikten, var det ikke mulig for lokomotivførerne å oppdage signal A 357 på Slependen blokkpost før toget var like foran Slependen holdeplass.

Det ble i etterkant av disse to alvorlige hendelsene kjent at lokomotivføreren i flytog 3816 søndag 17. april kl. 0112, tidligere i samme uke som de to alvorlige hendelsene skjedde, hadde meldt fra til togleder om tilsvarende signalobservasjon med forsignalet på signal N 4323 på Sandvika stasjon. Havarikommisjonen har ikke mottatt melding om denne hendelsen, og er heller ikke kjent med at dette tilfellet er blitt rapportert videre fra togledelsen internt i Jernbaneverket.

1.2 Personskade

Det ble ikke rapportert noen personskader ved disse alvorlige hendelsene. Havarikommisjonen har fått opplysninger om at lokomotivføreren i tog 12207 etter hendelsen en tid har vært sykmeldt og fått fysikalske behandling for muskulære plager.

1.3 Skader på involvert materiell

Det oppstod ingen materielle skader på det rullende materiellet ved noen av disse alvorlige hendelsene.

1.4 Skadebeskrivelse av infrastruktur og kjørevei

Det oppstod ingen materielle skader på kjørevei eller andre deler av infrastrukturen ved noen av disse alvorlige hendelsene.

1.5 Andre skader

Det oppstod ingen andre skader på tredjeparts eiendom ved noen av disse alvorlige hendelser.

1.6 Personellinformasjon

Ikke relevant for disse hendelsene.

1.7 Rullende materiell

De involverte togene i de to alvorlige hendelsene var:

Hendelse 1: To motorvognsett type 71 (flytog).

Hendelse 2: Motorvognsett type 71 (flytog) og lokaltog type 69 D (NSB tog).

1.8 Infrastruktur og kjørevei

Sandvika stasjon ligger på den fjernstyrte dobbeltsporstrekningen mellom Oslo S og Drammen. Sportraséen ligger i kurvatur på strekningen mellom Sandvika – Slependen – Billingstad. Siktavstand fram til hovedsignaler skal i følge Jernbaneverkets regelverk JD 551 være slik at signalet er synlig de siste 250 meter fram til signalet. Siktavstanden til blokksignal A på Slependen blokkpost ble kontrollert, og det viste seg at den var nøyaktig på 250 meter. For øvrig var sikten til signalene noe redusert på grunn av en kontaktledningsmast som var plassert noen meter foran signalet.

Det var tre signalmontører på vakt den aktuelle dagen. To var på Oslo S og en på Asker stasjon. Det rykket ut en signalmontør fra Oslo S og en fra Asker stasjon da de fikk melding fra togleder om feil på forsignal på Sandvika stasjon. Anlegget ble resatt for å få kvittert ut feilen. Havarikommisjonen er gjort kjent med at det har vært gjentatte tilfeller av feil ved anlegget på Sandvika stasjon. Dette har man løst ved å kvittere ut feilen ved å resette stillverket. Feilene bestod vanligvis i at forsignalet gikk til en restriktiv tilstand på grunn av elementsperre. Dette var en feil som oppstod ofte, men som ikke var sikkerhetskritisk. Havarikommisjonen registrerte at det var utført provisoriske koblinger, samt montert opp registrerende måleutstyr for å fange opp denne feilen både på blokkposten og i stillverket på Sandvika stasjon.

1.9 Været

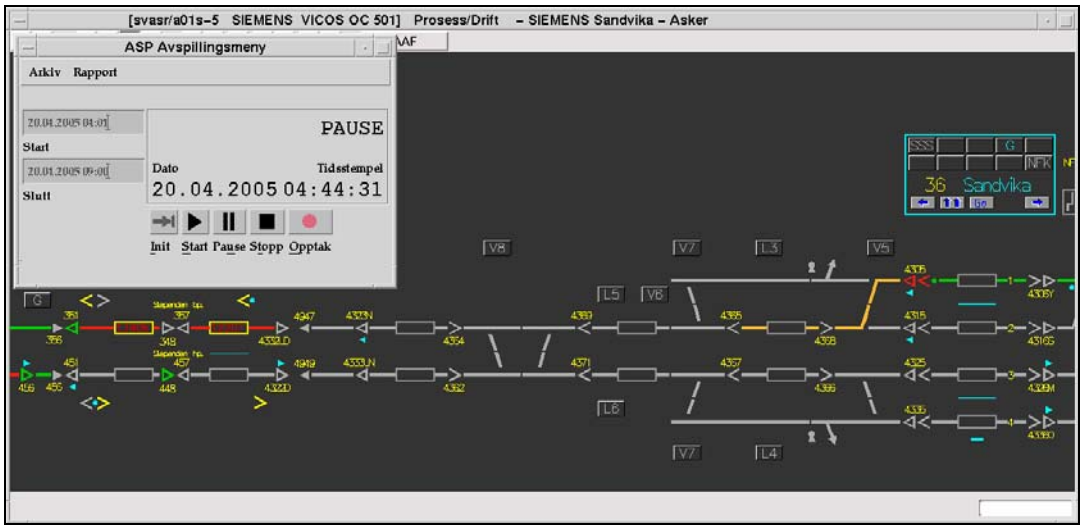
Hendelsene inntraff tidlig om morgenen. Det var skumring, været var klart og det var ikke nedbør.

1.10 Trafikkledelse og signalsystem

Driftsformen på Sandvika stasjon er strekning med fjernstyring. Sandvika stasjon inngår i den fjernstyrte strekningen Oslo S – Drammen. Strekningen Oslo S – Asker stasjon er fjernstyrt fra trafikkstyringssentralen på Oslo Sentralstasjon. Stillverket kan automatkobles slik at signalene stilles automatisk for tog inn og ut i togsporene.

Signalanlegget på Sandvika stasjon er et elektronisk datastillverk av type SIMIS C.

Strekningen er utstyrt med automatisk togstopp, delvis utbygd ATC (DATC), og med fullt utbygd ATC (FATC) på Sandvika stasjon.

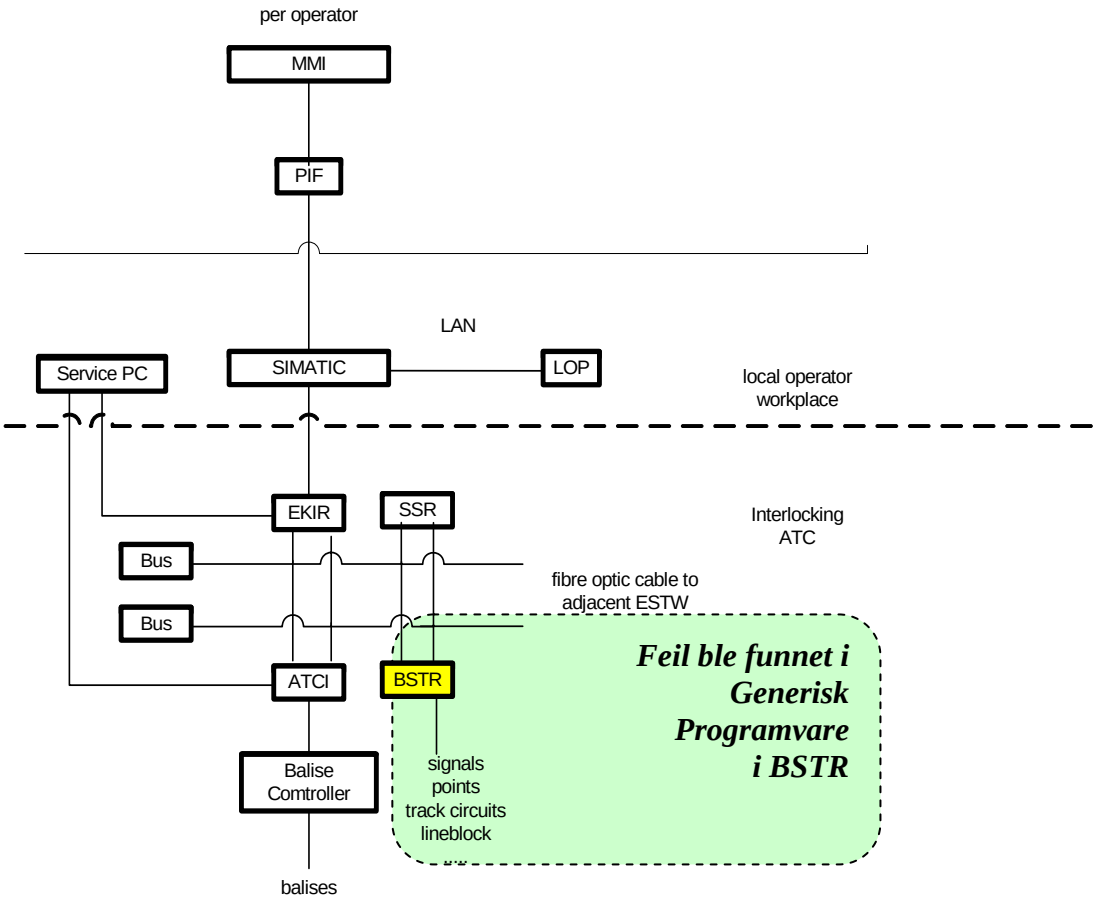


Figur 7: Viser utskrift av logg fra den andre alvorlige hendelsen, kl. 04:44:31, hvor tog 13905 og 12207 står på hver sin side av Slependen blokkpost.

1.10.1 Stillverk

Sandvika stasjon er utstyrt med sikringsanlegg som er et elektronisk datastyrt stillverk. Dette sikringsanlegget ble tatt i bruk sommeren 2004.

Stillverket som styrer utkjørhovedsignal N 4323 på Sandvika er av typen SIMIS-C levert av Siemens. Dette sikringsanlegget er et elektronisk datastyrt stillverk med en overordnet konfigurasjon som vist skjematisk i figur 8.



Figur 8: Viser hvor i datastillverket feilen ble identifisert

Beskrivelse over begrepene i figur 8.

- MMI Man Machine Interface (brukergrensesnitt)
- PIF Process InterFace
- SIMATIC Betegnelse for Siemens PLS
- LOP Lokal Operatør Plass
- EKIR Eingabe Kommunikation Inpretator Rechner. (hovedregnermaskin)
- SSR Schnitt Stell Rechner. (Interface computer)
- Bus Databus for sikringsanlegget
- BSTR Kommunikasjonsenhet med objektstyreenheter. (Områdecomputer)
- ATCI Automatic Train Controll Interface. (For styring av ATC baliser)

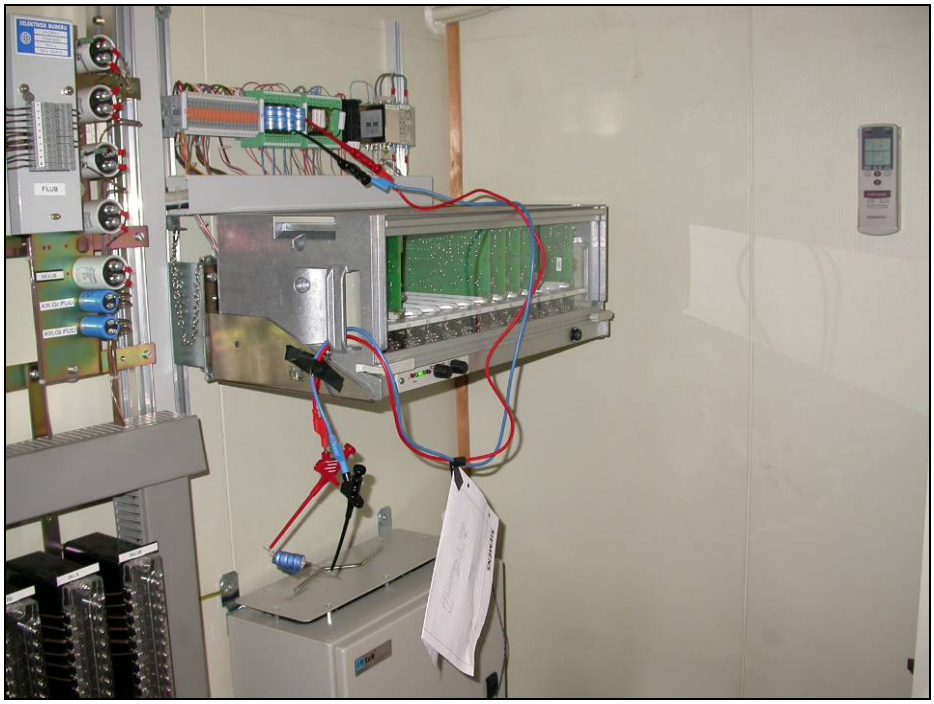
SIMIS-C består i hovedsak av en sentralmaskin (EKIR) med sentral forriglingslogikk. Denne kommuniserer med objektstyreenheter (BSTR) via en databus. BSTR inneholder både generisk- og applikasjonsprogramvare for å styre ytre objekter, blant annet signaler og grensesnitt mot linjeblokk. ATCI får ATC informasjon fra EKIR og legger ut informasjonen i balisene. SSR utveksler statusindikasjon og informasjon om objekttilstander.

Årsaken til feilsituasjonen på Slependen ble funnet i den generiske programvaren i BSTR. Denne programvaren ble utviklet for SIMIS-C på Gardermobanen (GMB) og var ikke gjenstand for egen validering og godkjenning i forbindelse med Sandvikaprosjektet.

1.10.2 Linjeblokk inklusive grensesnitt

Billingstad blokkpost er av typen standard 3-begreps relélinjeblokk.

Hoved- og forsignalbeskjed til/fra blokkpost overføres via relékoblinger og EF 180 transmisjonssystem (se figur 9) som er en transparent overføring av reléinformasjon til SIMIS-C-anlegget. I disse tilfellene viste blokksignal A 357 signal ”stopp” samtidig med at tilhørende forsignal på utkjørsignal 4323N viste signal ”vent kjør”.



Figur 9: Grensesnitt system EF 180 på Slependen blokkpost. Dette overfører signalinformasjonen mellom reléanlegget på blokkposten og datastillverket på Sandvika stasjon via en telekommunikasjonskabel.

1.10.3 Feilbeskrivelse teknisk

Feilen i stillverket oppsto i hovedsak som følge av en programmeringsfeil i den generiske programvaren i BSTR til sikringsanlegget.

En serie med hendelser inntraff i en bestemt rekkefølge i prosessen. Dette førte til at et feilaktig signalbilde i forsignalet som gjaldt for Slependen blokkpost oppstod. Dette forsignalet var plassert på utkjørhovedsignal N 4323’s mast på Sandvika stasjon. Det ble

ikke tatt høyde for den aktuelle kombinasjonen av hendelser under testene av anlegget før ibruktaging.

De fire feiltilstandene som gjorde at feilen ble synliggjort var:

1. Signalanlegget fikk en ”elementsperre” i et GUET element (normalt ikke sikkerhetskritisk) på den delen av anlegget som behandler informasjonen fra grensesnittet mot blokkposten på Slependen. Elementsperre fås normalt når informasjonen av data ikke tolkes korrekt. I dette tilfellet, hvor det var feil i programvare, gikk ikke anlegget til en sikker tilstand, selv om elementsperren inntraff.

2. Etter at den første feilmeldingen oppsto, mottok anlegget en ny feilmelding. Filamentfeil (en avbrent lampetråd) fra motrettet signal innkjørhovedsignal UD 4332. Dette er motrettet signal til utkjørhovedsignal N 4323 på Sandvika stasjon.

3. Deretter ble den aktuelle BSTR (områdecomputeren med programvare som behandler informasjon til/fra grensesnittet mot Slependen blokkpost), resatt. Dette ble utført av vakthavende signalpersonale.

4. Samtidig med at BSTR (se fig. 10) ble resatt viste blokksignal A 357 på Slependen blokkpost signal ”vent kjør”.

   Når disse fire kriteriene var oppfylt i rekkefølgen beskrevet over, låses signalanlegget og styringen av forsignalet i den status det hadde ved resettingen av anlegget, nemlig ”kjøretillatelse” i forsignalet for blokksignal A 357. Dette skjedde som følge av feil i generisk programvare til BSTR.

Figur 10: Bilde av objektkontroller til signal N 4323

1.10.4 Kontroll av stillverk

Umiddelbart etter at de to alvorlige hendelsene hadde inntruffet, ble det i samarbeid med representanter fra Jernbaneverket, Flytoget, NSB og havarikommisjonen foretatt kontroll av stillverket, med kunstig simulering av togkjøring. Denne kontrollen klarte ikke å provosere frem feilen. Senere ble stillverket simulert med realistisk togkjøring, men heller ikke disse testene klarte å provosere frem feilen. Ettersom usikkerheten rundt

grensesnittet (EF 180) til stillverket var reell, ble det besluttet at alle grensesnitt på stillverk som hadde samme type system skulle settes ut av drift inntil videre. Granskingen av programvaren til SIMIS-C anlegget hos Siemens i Braunschweig avdekket etter hvert feilen i programvaren.

Havarikommisjonen har registrert at Jernbaneverket, i samarbeid med Siemens, har hatt en åpen og positiv prosess der man har holdt NSB og Flytoget fortløpende informert om de funn som er gjort i denne saken.

1.11 Kommunikasjonskanaler

Pågående arbeider eller forhold ved infrastrukturen som berører togfremføringen bekjentgjøres til personalet gjennom T-sirkulærer. Disse utgis av toglederområdene, utkommer ukentlig og er sortert på banestrekninger. Andre forhold knyttet til togfremføringen bekjentgjøres på S-sirkulære som utarbeides av trafikkansvarlig instans i Jernbaneverket og utgis for ruteområdene.

Det var utgitt ordre og sirkulære som berørte sporarbeidene på strekningen, men dette hadde ikke direkte innvirkning for hendelsesforløpet.

Togsett type 69 og 71 var utstyrt med togradio og mobiltelefon.

Kommunikasjonen mellom flytogførerne og togledelsen foregikk over togradio, mens kommunikasjonen mellom flytogførerne/lokomotivfører og de driftsoperative sentrene foregikk over mobiltelefon.

1.12 Organisasjoner og ledelse

1.12.1 Lover og forskrifter

Lover og forskrifter i denne sammenheng er:

- Lov av 11. juni 1993 nr. 100 om anlegg og drift av jernbane, herunder sporvei, tunnelbane og forstadsbane m.m. (jernbaneloven),
- Forskrift av 4. desember 2001 nr. 1334 krav til jernbane, herunder sporvei, tunnelbane og forstadsbane m.m. (kravforskriften).
- Forskrift av 5. februar 2003 nr. 136 tillatelse til å drive jernbane, herunder sporvei, tunnelbane og forstadsbane m.m. samt tilgang til å trafikkere det nasjonale jernbanenettet (tillatelsesforskriften).
- Forskrift av 18. desember 2002 nr. 1679 om opplæring av personell med arbeidsoppgaver av betydning for trafikksikkerheten ved jernbane, herunder sporvei, tunnelbane og forstadsbane m.m. (opplæringsforskriften).

Disse spesifiserer overordnede krav og reguleringer for de som driver og opererer jernbane i Norge.

Kravforskriftens kapittel 2 beskriver de overordnede prinsipper for arbeid med trafikksikkerhet. I denne står det at det skal arbeides for kontinuerlig forbedring av trafikksikkerheten, og for reduksjon av risiko så langt det med rimelighet er gjennomførbart. Det skal også etableres barrierer mot alvorlige konsekvenser av enkeltfeil (enkeltfeilprinsippet).

Kravforskriftens kapittel 5, § 5-1, del en, 2. og 4. ledd beskriver de krav som stilles til bruk av analyser og kriterier for akseptabel risiko.

Kravforskriftens kapittel 11 omhandler krav til drift av kjørevei. § 11-3, beskriver krav om utarbeidelse av sikringsprinsipper, § 11-4, beskriver krav til kontrollrutiner for signal- og sikringsanlegg. §11-5, beskriver krav til teknisk dokumentasjon. §11-6, beskriver krav til vedlikehold.

Kravforskriften er etter hendelsen erstattet av forskrift av 19. desember 2005 nr. 1621 om krav til jernbanevirksomhet på det nasjonale jernbanenettet (sikkerhetsforskriften).

Tillatelsesforskriften er erstattet av forskrift 16. desember 2005 nr. 1490 om lisens, sikkerhetssertifikat og om tilgang til å trafikkere det nasjonale jernbanenettet, samt om sikkerhetssertifikat for å drive infrastruktur (lisensforskriften) på det nasjonale jernbanenettet.

Denne rapporten er kommentert ut fra kravforskriften fra 2001, da det var denne som var gjeldende da de alvorlige hendelsene inntraff.

Prosjektering. bygging og idriftsetting av elektroniske datastillverk skal utføres i henhold til CENELEC standardene EN 50126, -128 og -129.

1.12.2 Operative regler

JD 500-serien er Jernbaneverkets tekniske regelverk og beskriver blant annet generelle tekniske krav om signal - bygging, prosjektering og vedlikehold.

1.12.3 Arbeidsorganisasjon og ordreveier

Sandvika stasjon er underlagt Oslo toglederområde. Banesjefen er eier av anlegget, og har ansvaret for at dette alltid er i forskriftsmessig stand. Det er inngått en drifts- og vedlikeholdsavtale mellom banesjefene og Drift som beskriver roller og ansvar. For Banesjefen er dette ivaretatt ved at Faglig leder signal og oppsynsmenn har ansvaret for at de generiske rutinene (visitasjon og kontroller) blir gjennomført. Dette innebærer at de skal ha oversikt over anleggets tilstand, analysere tilstanden, synliggjøre behov og prioritere aktiviteter, samt bestille oppdrag fra Drift og for å følge opp disse. Dette innebærer at det er Jernbaneverkets eget personale som gjennomfører kontroller og visitasjoner, samt drifts- og vedlikeholdsoppgaver.

1.12.4 Kompetansekrav for personale

Personalet som utfører service og feilretting på de forskjellige typer av signalanlegg (også det elektroniske datastillverket SIMIS C) må ha utdannelse som signalmontør. Havarikommisjonen er kjent med at det kan forekomme at signalpersonalet settes til feilretting på nye og kompliserte anleggstyper, uten at de føler at de har fått tilstrekkelig opplæring til å utføre slike arbeider. Dette var også tilfellet ved de aktuelle hendelsene.

1.12.5 Resetting av anlegg

Feil som blir stående i anlegget over tid er ugunstig. For å opprettholde anleggets sikkerhetsnivå er det forutsatt en kort responstid for feilretting. Dersom dette ikke overholdes, kan det føre til fare for at samtidige feil i anlegget kan oppstå, noe som kan påvirke sikkerhetsnivået. Leverandøren av anlegget mener at de sikkerhetsrelaterte

anvendelsesbetingelser og forutsetninger ikke overføres på en tilfredsstillende måte fra prosjektet til driftsorganisasjonene, og at signalpersonalet som vedlikeholder anleggene dermed ikke er godt nok kjent med disse forutsetningene. Det er viktig at personalet får hurtig, korrekt og utfyllende feilinformasjon fra togleder før inngrep og eventuell resetting av anlegg blir foretatt.

1.12.6 Rutiner for intern-kontroll og oppfølging

Det er Jernbaneverkets banesjef for den aktuelle strekningen som har den daglige kontrollen av banestrekningen. Det er Jernbaneverkets eget signalpersonale som mottar første varsel fra togleder om feil, og som skal sørge for at feilen i stillverket blir rettet.

1.12.7 Rutiner for styring av entreprenører.

Siemens hadde totalentreprise på levering av sikringsanlegget. Jernbaneverket hadde overlatt leveransen av anlegget til Siemens, men utførte tester underveis i leveransen sammen med leverandøren. Jernbaneverkets personale foretok selv den endelige driftsprøven av sikringsanlegget før det ble satt i drift.

1.12.8 Håndbøker og materiellprosedyrer

Det var ikke utarbeidet prosedyrer for resetting av denne type sikringsanlegg på tidspunktet som de alvorlige hendelsene inntraff. Havarikommisjonen har fått opplysninger om at prosedyrer for resetting av datastillverk er utarbeidet i ettertid.

1.12.9 Normer for prosjektering og konstruksjon, (Standarder)

Gardermobanen (GMB):

Utvikling, prosjektering og bygging av sikringsanlegget skulle, etter kontrakten mellom Siemens og GMB-prosjektet, gjennomføres i henhold til CENELEC standardene EN 50126, -128 og -129. Standardene var på dette tidspunkt i preliminære utgaver.

Følgende versjoner av standardene er identifisert i GMB-avtalen (Kontraktnr 1836 – Signalanlegg for Gardermobanen):

- Draft pr EN 50126
- Draft pr EN 50128
- pr EN 50129

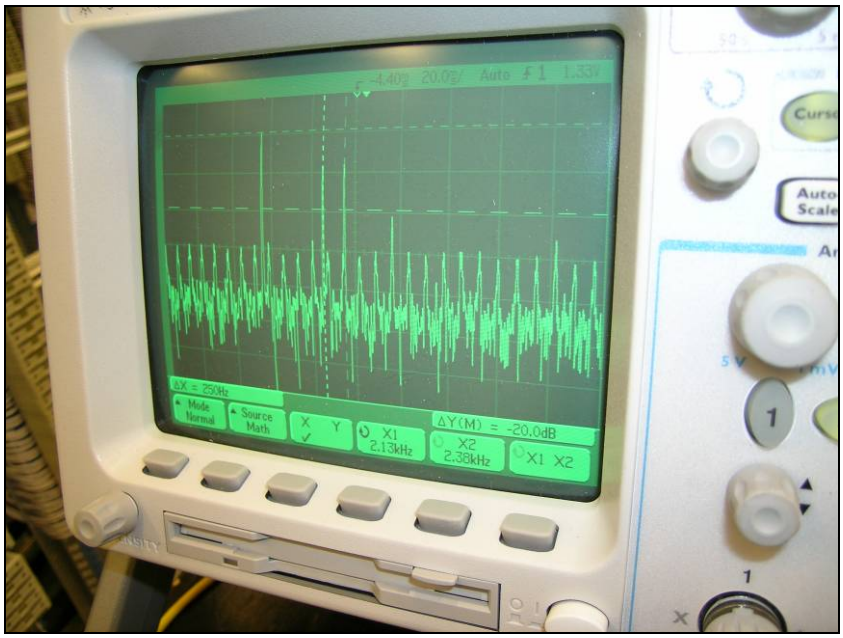
SIMIS-C er i utgangspunktet utviklet i henhold til MÜ 8004 (fra 1997 i henhold til Safety Case ESTW) som er en produktorientert standard. Det er beskrevet i sikkerhetsdokumentasjonen for Gardermobanen at programvareendringene i forbindelse med tilpasning til Gardermobanen i SIMIS-C er gjort i henhold til EN 50128.

Sandvika-Asker:

Sikringsanlegget på strekningen Sandvika – Asker skulle utvikles, prosjekteres og bygges i henhold til CENELEC-standardene EN 50126, -128 og -129. Anlegget skulle baseres på det generiske systemet utviklet for Gardermobanen, og man ønsket i utgangspunktet å unngå endringer i dette. Det var derfor RAMS-fasene som dekket prosjektering og bygging som var relevante for dette prosjektet.

1.12.10 Regler for vedlikehold av infrastruktur

Jernbaneverkets tekniske regelverk JD 552 beskriver vedlikehold - Signal på Jernbaneverkets infrastruktur.



Figur 11: Oscilloscopemåling av støyforhold fra kabel til grensesnitt EF-180

Det ble i løpet av havarikommisjonens undersøkelse observert unormal blinkfrekvens på lysdiodene i grensesnittsystemet EF-180. Under testmålinger ble det konstatert at det var varierende støy på grensesnittet mot Slependen blokkpost (se fig. 11). EF-180 er et grensesnitt for overføring av signalinformasjon mellom sikringsanlegget på blokkposten og stillverket på stasjonen. Havarikommisjonen har fått opplysninger om at telekabelen som er benyttet for overføring av data er skjøtet sammen av nye og eksisterende kabler.

Dette grensesnittet er ømfintlig for støy, og det er derfor viktig at kabler som blir benyttet mot dette grensesnittet har god standard. Dette riktignok ikke sikkerhetskritisk, men det kan skape driftsfeil ved at elementsperre opptrer. Slike forhold kan ha vært medvirkende til å provosere frem og synliggjøre programvarefeilen i stillverket.

1.12.11 Baliser/ATC

Baliser på delvis utstyrte områder (DATC) er styrt av signalene på strekningen. Balisene på fullt utrustede ATC områder (FATC) er styrt av prosessen i datamaskinen til det elektroniske stillverket. Grensesnittet mellom fullt utrustet ATC område og delvis utrustet ATC område var i dette tilfellet ved utkjørhovedsignal N 4323 på Sandvika stasjon.

1.12.12 Togledersentral og trafikkledelse.

Trafikkstyringssentralen som styrte Sandvika stasjon er plassert på Oslo sentralstasjon.

Årsaken til at det ikke ble respondert tidligere på feilmeldingen fra fører av flytog 13905 var at toglederne på vakt var i tvil om at det virkelig kunne være feil på sikringsanlegget. Videre ble ikke hendelse 2 umiddelbart innrapportert til toglederen av lokomotivføreren i tog 12207. Etter hvert ble det likevel bestemt at signalbildene skulle testes ved en ny togpassering. Fører på Flytog 13907 fikk beskjed om å observere signalbildet på signal N 4323 i det toget passerte. Det viste seg at denne observasjonen stemte med tidligere innrapporteringer om feilaktig signalbilde. På dette tidspunkt ble signalvakta kontaktet og to mann reiste umiddelbart til Sandvika stasjon og resatte anlegget.

Det hadde tidligere oppstått uklarheter rundt hvordan disponering for videre kjøring av flytog 13905 skulle skje, siden togleder ikke var involvert i telefonsamtalen mellom flytogfører og operativ leder flytog og de valg som ble tatt. Det er viktig å presisere at det er togleder som har ansvaret for trafikkavviklingen.

1.12.13 Lokfører/flytogfører

Havarikommisjonen har hatt samtale med lokomotivføreren i NSB-tog 12207. Opplysninger fra flytogførerne er innhentet fra samtaleloggen ved trafikkstyringssentralen på Oslo sentralstasjon.

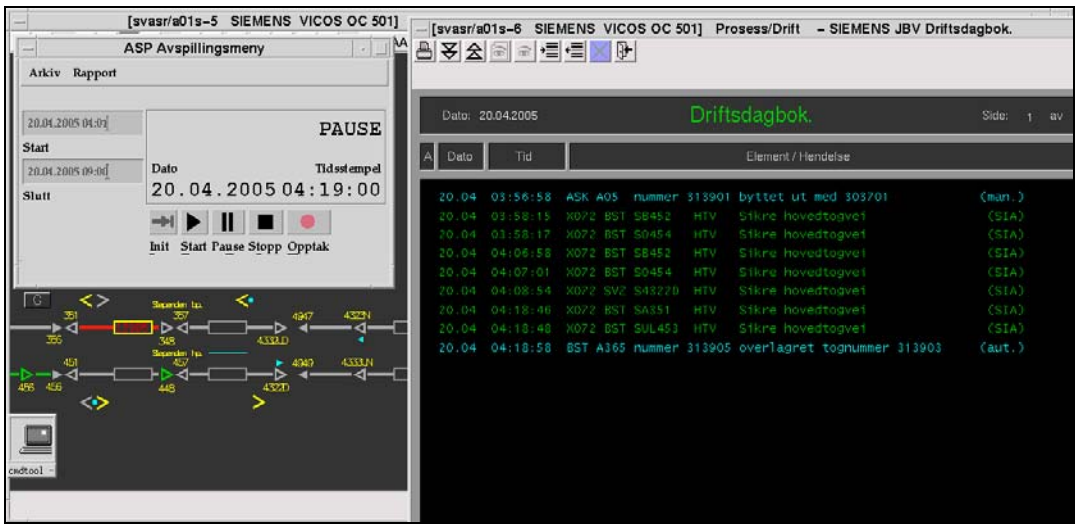
1.13 Registrerende hastighetsmålerutstyr og datalogger

1.13.1 Samtalelogg/telefonlogg

Samtalelogg ble avspilt i trafikkstyringssentralen på Oslo S sammen med Jernbaneverkets uhellskommisjon.

1.13.2 Signallogg

Det ble etter hendelsene tatt ut logg av de forskjellige togbevegelser før, under og etter de alvorlige hendelsene. Feilen i stillverket på Sandvika stasjon ble ikke identifisert ved hjelp av disse loggene, men utskriftene var et godt hjelpemiddel for å fastslå tidspunktet for hendelsene og bevegelsene i stillverket.



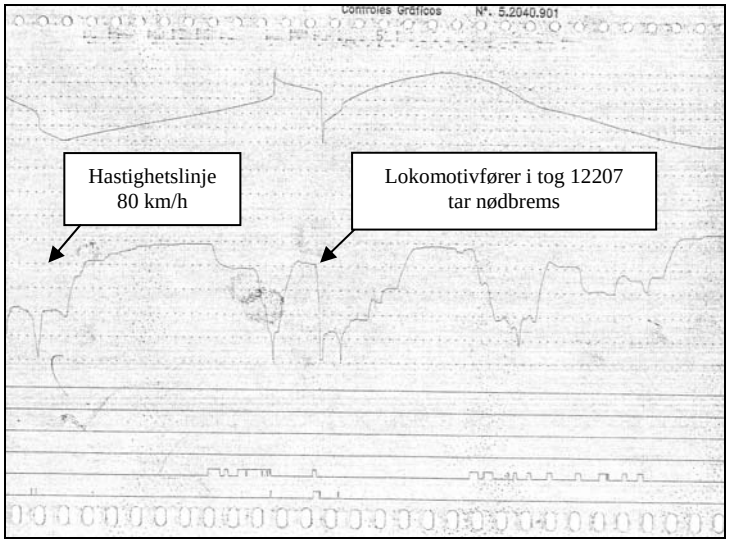
Figur 12: Utskrift av signallogg

På utskrift av signallogg i figur 12 vises tidspunktet for når tog 13905 kjørte inn på samme blokkstrekning som tog 13903, og visningen av tognummer på skjermen blir lagt oppå hverandre.

1.13.3 Registrerende hastighetsmålere på tog

Tog 12207:

Utskrift av registrerende hastighetsmåler (Hasler) for tog 12207 viser at toget hadde en hastighet på nærmere 82 km/h like før lokomotivføreren tok nødbrems.



Figur 14: Hastighets utskrift (Hasler) av tog 12207

Flytog 13905:

Teloc utskrift fra flytog 13905 viste at toget hadde en hastighet på 80,45 km/h i det toget passerte blokksignal A 357 på Slependen blokkpost i signal ”stopp”. Flytogføreren hadde

aktivisert nødbremsen før toget passerte signalet. I annet fall ville togets ATC system stoppet toget da det passerte blokksignalet i stopp.

1.14 Medisinske forhold

Ikke relevant for noen av disse hendelsene.

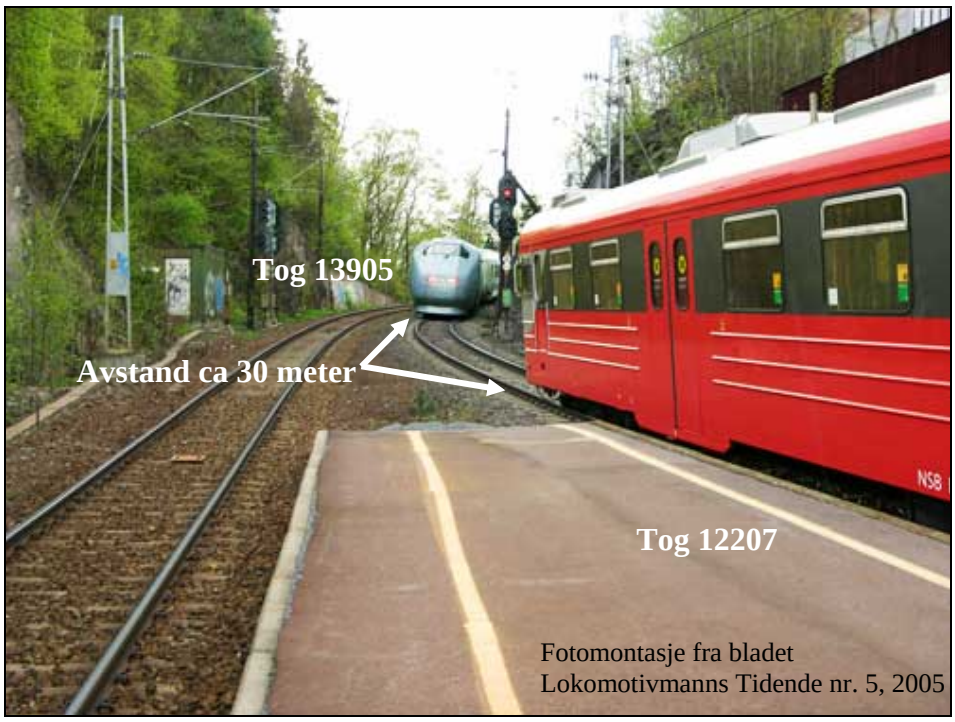
1.15 Brann

Det oppstod ikke brann ved noen av disse hendelsene.

1.16 Overlevelsesaspekter

Det kunne fått alvorlige konsekvenser hvis lokomotivføreren i tog 12207 ikke hadde foretatt nødbrems og klart å stoppe toget i tide. Han hadde kun et tidsvindu på omtrent 2 sekunder til å oppdage flytogets 2 røde retningslys (sluttsignaler) i området til venstre for overbygget på Slependen holdeplass. Dette illustreres på figur 15.

Figur 15: Siktlinjen fra lokomotivets førerhytte i retning Slependen blokkpost. Flytog 13905 hadde stoppet og befant seg bak overbygget på Slependen holdeplass.



Figur 16: Togenes stopposisjoner etter hendelse 2

1.17 Undersøkelser

Havarikommisjonen har foretatt egne undersøkelser av hendelsene. I tillegg har det blitt benyttet eksterne konsulenter som har gjennomgått sikkerhetsdokumentasjonen som er beskrevet i vedlegg, samt relevante godkjenningsprosesser.

1.17.1 Undersøkelse rundt utvikling, prosjektering og bygging av sikringsanleggene.

Det ble konstatert at feilen i sikringsanlegget (SIMIS-C) på Sandvika stasjon var knyttet til en generisk programvaremodul som ble utviklet i forbindelse med tilpasning av sikringsanlegget ved byggingen av Gardermobanen. Det er derfor valgt to ulike tilnærminger i undersøkelsen:

- gjennomgang av prosessen for utvikling og tilpasning av det generiske systemet i SIMIS-C for Gardermobanen for å finne bakenforliggende årsaker til at feilen kunne oppstå

- gjennomgang av prosessen i forbindelse med prosjektering og bygging av nytt sikringsanlegg (SIMIS-C) på Sandvika stasjon for å vurdere om man kunne ha identifisert feilen før idriftsettelse av anlegget.

Undersøkelsene er gjennomført som en kombinasjon av dokumentgjennomgang og samtaler med involverte personer. Dokumentasjon er innhentet fra leverandøren (Siemens), Jernbaneverket og Sintef. Det har vært gjennomført samtaler med personell hos leverandør og Jernbaneverket. I tillegg har det vært gjennomført samtaler med personell som var involvert i GMB-prosjektet, inklusive Sintef som assessor.

Dokumentasjon som er gjennomgått er listet i dokumentlisten, Vedlegg 1.

Tilpasning av SIMIS-C for Gardermobanen

Det er i avsnittene nedenfor beskrevet en del forhold som er undersøkt og som kan ha hatt innvirkning på prosessen med tilpasning av SIMIS-C for Gardermobanen.

Kontraktsforhold / prosjektorganisering

Kontrakten på Gardermobanen (GMB) var organisert som en totalleveranse der leverandøren var ansvarlig for komplett leveranse av signal- og sikringsanlegg, inklusive fjernstyring og ATC.

Man valgte, for GMB, å benytte kontraktsstandarden NF92 som er en totalentreprisekontrakt. Det var første gang man benyttet denne type kontraktsstandard for signalleveranser, og verken byggherre eller leverandør hadde erfaring med bruk av denne. Det ble i starten av prosjektet forventet at leverandøren skulle levere et ferdig anlegg uten særlig involvering fra GMB-prosjektets side. Man så imidlertid etter hvert at prosjektet i større grad ble nødt til å involvere seg i leverandørens prosess underveis. Dette for å sikre at det ferdige produktet tilfredstilte Gardermobanens og Jernbaneverkets krav, spesielt funksjonelle krav, og for å holde fremdriften i prosjektet.

Denne involveringen ble i hovedsak gjort uten noen form for formell granskning eller godkjenning, men ble ifølge de som var involvert i prosjektet til en viss grad dokumentert i møtereferater.

Prosjektet var under sterkt tidspress for å få anlegget ferdig til åpningen av Oslo lufthavn Gardermoen.

Spesifikasjoner

Spesifikasjonene som var vedlegg til kontrakten var på norsk. Disse ble oversatt til engelsk og tolket av leverandøren som benyttet tysk som arbeidsspråk. Avklaringer fra Jernbaneverket ble også oversendt på norsk til leverandøren. Underlag for utvikling av grensesnittet mot relélinjeblokk i GMB-prosjektet var i hovedsak basert på reléskjemaer.

I og med at kravspesifikasjonen var på norsk, ble det engasjert et oversettelsesfirma for å oversette den til engelsk. Oversettelsen manglet den faglige forankringen og dette ble derfor ”ikke en god prosess” (uttalt fra assessor). Når det gjaldt avklaringer ble disse oversatt av Siemens’ egne folk i Norge.

Reléskjemaene ble tolket av leverandørens ressurspersoner i Tyskland og funksjonene implementert i systemet. Leverandøren gikk sammen med Gardermobanens personell gjennom funksjonene underveis i prosjektet for å sikre mest mulig korrekt funksjonalitet.

Når det gjelder linjeblokkfunksjonaliteten spesielt, var erfaringen i GMB-prosjektet at leverandørens personell som utførte arbeidet med utvikling og implementering av dette var svært kompetente, og hadde erfaring fra utvikling av lignende funksjonalitet hos andre infrastrukturforvaltninger. Dette gjorde at arbeidet ble gjennomført uten vesentlige endringer eller kommentarer fra Gardermobanen eller Jernbaneverket.

Det viste seg etter hvert i prosjektet at det var nødvendig med en utvidet og bedre dialog for at leverandørens løsning skulle tilfredsstille kundens krav. Dette ble i første rekke håndtert via arbeidsmøter og dokumentert i møtereferater og ved formelle avklaringer i brevs form og i endringsordre. I ettertid så man at denne fasen med fordel kunne vært gjennomført med en grundigere og mer formell gransking av leverandørens designdokumenter før utviklingen startet. I ettertid er det uttalt at en da kunne ha unngått mange av de uklarheter som kom under FAT (”Functional Acceptance Test”).

RAMS-prosess

SIMIS-C er et velprøvd sikringsanlegg som er utviklet før EN 50126, -128 og -129 standardenes tid. Tilpasning av SIMIS-C for Gardermobanen skulle, i henhold til kontrakten mellom Siemens og Gardermobanen, skje i henhold til EN 50126, -128 og -129 standardene.

EN-standardene var, på det tidspunktet avtalen i forbindelse med Gardermobanen ble inngått, i foreløpige versjoner. De var gjenstand for mindre endringer under prosjektets gang før de etter hvert forelå i dagens endelige utgaver.

På tidspunktet for gjennomføring av prosjektet hadde leverandøren ikke implementert EN 50126, -128 og -129 standardene fullt ut i sin utviklingsprosess, men var i en overgang fra MÜ 8004 til EN-standardene.

MÜ 8004 er en produktorientert standard hvor man fokuserer på å bygge sikre systemer av sikre delsystemer/komponenter. MÜ 8004 stiller også krav til hvordan programmering og dokumentasjon av programvare i sikkerhetssystemer skal utføres.
EN-standardene er mer prosessorienterte standarder som har større fokus på en analytisk tilnærming. Når det gjelder Safety Case har EN-50129 adoptert strukturen for teknisk sikkerhetsrapport fra MÜ 8004.

Safety Case for ESTW (SIMIS-C) på Gardermobanen sier at endringer i programvaren ble utført i henhold til EN 50128. Den sier også at en fulgte EN50126 i utviklings- og valideringsprosessen av endringene i den generiske delen, samt applikasjonsdelen.

Hasardanalyser er en viktig del i den risikobaserte prosessen beskrevet i EN-standardene, og skal gjennomføres i alle faser av prosjektet, allerede fra konseptutviklingsfasen. Det ble ikke gjennomført noen hasardanalyse i GMB-prosjektet i løpet av de første fire fasene av livssykelprosessen beskrevet i EN50126. Det er totalt identifisert 3 hasardanalyser i GMB-prosjektet:

- System Hazard Analysis
- Functional Hazard Analysis ATC
- Operating Hazard Analysis

”Feil input/output i BSTR” er behandlet i System Hazard Analysis, men kun på et overordnet nivå. Analysen går ikke inn på enkeltmoduler, delsystemer eller utviklingsprosessen. Den har heller ikke spesielt fokus på grensesnittene. Det ser også ut til at analysen ble gjennomført i etterkant av utviklingen, og ikke i forkant slik standarden legger opp til.

Kombinasjonen av de feilmodi og hendelser som førte til den sikkerhetskritiske hendelsen på Slependen var ikke identifisert som en mulig kombinasjon i utviklingsprosessen (gjennom hasardanalyser eller testing).

Gjennom en prosess hvor leverandøren identifiserte avvik fra EN-standardene og hvor kunden og assessor vurderte det samme, kom man frem til at leverandørens sikkerhetsprosess var tilfredsstillende, selv om man ikke fulgte alle deler av EN-standardene. En viktig forutsetning for å akseptere leverandørens måte å gjennomføre prosjektet på var at Siemens benyttet en intern, uavhengig part til verifisering og validering (Prüfleitstelle).

Sandvika – Asker prosjektet

Den generiske delen av SIMIS-C (hvor feilen ble funnet) ble ansett som validert og godkjent og derfor ble ikke denne delen validert spesielt i forbindelse med SIMIS-C på Sandvika stasjon.

Prosjektering og bygging av nytt sikringsanlegg på Sandvika stasjon var en del av prosjektet Sandvika-Asker som også inkluderte nytt sikringsanlegg på Asker stasjon, samt på det nye dobbeltsporet mellom Sandvika og Asker.

Det generiske systemet på Gardermobanen ble først formelt godkjent (typegodkjent) av Jernbaneverket sommeren 2005. Bakgrunnen til at det ikke forelå noen formell godkjenning er oppgitt til å være formaliteter og ikke funksjonelle - eller sikkerhetskritiske mangler.

I leverandørens sikkerhetsplan for prosjektet defineres sikkerhetsstrategien slik:

- Identifikasjon av forskjell i krav mellom GMB-prosjektet og Sandvika – Asker
- Vise at løsningen for Gardermobanen oppfyller kravene
- Komme til enighet om en løsning med kunden

Leverandøren har gått gjennom alle kravene for Sandvika – Asker prosjektet og analysert om funksjonaliteten i det generiske systemet fra Gardermobanen tilfredsstiller kravene for Sandvika - Asker. Denne analysen er dokumentert i ”Safety Requirement Tracing Matrix” som konkluderer med at det ikke er nødvendig med endringer i det generiske systemet (funksjonene), kun i prosjekterte (anleggsspesifikke) data.

På bakgrunn av at det ikke ble gjort endringer i det generiske systemet (funksjonene), ble det i den videre sikkerhetsprosessen fokusert på de anleggsspesifikke endringene fra Gardermobanen. Dette er bl.a. dokumentert i leverandørens plan for verifikasjon og validering.

Det var verken i den generiske sikkerhetsdokumentasjonen eller vedlikeholdsmanualene for systemet lagt begrensninger knyttet til de funksjoner/tilstander som er knyttet til den aktuelle feilsituasjonen (elementsperre, ”restart” av BSTR, filamentfeil, eller kombinasjoner av disse).

1.18 Nyttige undersøkelsesmetoder

Det er ikke utført undersøkelser som krever spesiell omtale.

2. ANALYSE

Forut for analysen av hendelsen har SHT samlet inn faktaopplysninger og gjort undersøkelser både i forhold til implementering av nytt sikringsanlegg på Sandvika stasjon og utviklingsprosessen av det generiske systemet for SIMIS-C sikringsanlegget på Gardermobanen.

Parallelt med dette har Jernbaneverket og leverandøren Siemens foretatt sine undersøkelser for å finne årsakene til feilen. Den direkte årsaken til hendelsen på Slependen er beskrevet i dokumentasjonen fra Jernbaneverket og leverandøren. Etter at feilen ble funnet har leverandøren gjennomført oppgradering av de berørte anleggene både på Sandvika og Gardermobanen, og Jernbaneverket har testet og idriftsatt anleggene. Det er i forbindelse med undersøkelsene gjennomgått og bekreftet at feil er funnet, retting i programvare er utført, og at endringen er testet, dokumentert og vurdert.

Undersøkelsene er derfor ikke gjort med henblikk på å finne årsaken til at blokksignalet viste ”stopp” samtidig som tilhørende forsignal viste ”vent kjør” i og med at feilen var funnet. Undersøkelsene er gjort med henblikk på å finne den bakenforliggende årsaken til at feilprogrammeringen kunne ”overleve” en verifikasjon og valideringsprosess gjort i forbindelse med Gardermobanen og Sandvika stasjon.

Analysen tar for seg både utviklingen av det generiske systemet som skjedde i forbindelse med Gardermobanen, samt implementeringen på Sandvika stasjon.

2.1 Tekniske og operative årsaksfaktorer

2.1.1 Tilpasning av SIMIS-C for Gardermobanen

Denne delen av analysen er rettet mot utviklingsprosessen for sikringsanlegget som skjedde i forbindelse med GMB-prosjektet. Spesielt er analysen rettet mot den delen av sikringsanlegget hvor feilen ble lokalisert (grensesnitt mot linjeblokk).

Analysen er gjennomført med fokus på to forhold:

1. Å identifisere svakheter ved den prosessen som ble gjennomført ved utviklingen av den aktuelle programvaren

og på basis av dette

2. evaluere om prosesser og metoder beskrevet i EN 50126, -128 og -129 - standardene kunne ha redusert sannsynligheten for å få tilsvarende feil.

Kontraktsforhold/prosjektorganisering

Kontrakten på Gardermobanen (GMB) var organisert som en totalleveranse der leverandøren var ansvarlig for komplett leveranse av signal- og sikringsanlegg, inklusive fjernstyring og ATC.

Det er i de senere årene blitt gjennomført flere prosjekter med landstilpasning av sikringsanlegg i Jernbaneverket, og erfaringen fra disse er at det er absolutt nødvendig med en sterk involvering fra kunden for å få en felles forståelse av både krav og funksjonalitet. Dette ble også bekreftet av de samtaler som ble gjennomført med personell som var involvert i GMB-prosjektet. Prosjektet innså at de måtte involvere seg mer underveis, selv om dette ikke var i henhold til intensjonene i avtalen med Siemens.

Det er imidlertid lite sannsynlig at en sterkere involvering fra Gardermobanens side fra starten av i GMB-prosjektet ville bidratt til å oppdage feilen i sikringsanlegget. Dette fordi det ikke kunne forventes at Gardermobanens ressurser skulle inneha den nødvendige kunnskap om interne feilsituasjoner og detaljer i programvaremoduler i systemet.

Driftsforhold

Personalet som arbeider med elektroniske datastillverk bør ha en god opplæring i denne type sikringsanlegg, da disse anleggene skiller seg fundamentalt fra konvensjonelle relébaserte sikringsanlegg som en signalmontør i hovedsak har sin utdannelse i. Havarikommisjonen finner det uheldig at det kun var et begrenset antall personer som hadde inngående kompetanse på feilretting av denne type stillverk i Jernbaneverket.

Havarikommisjonen er gjort kjent med at det etter hendelsene har foregått kursvirksomhet i regi av Siemens, for å oppdatere signalpersonalet på elektroniske datastillverk.

Togledelsen iverksatte ikke umiddelbare tiltak etter den første hendelsen. Havarikommisjonen vil påpeke viktigheten av at togledelsen raskt iverksetter nødvendige tiltak for å sikre togframføringen når det meldes om alvorlige feil på signaler.

Det ble i etterkant av de to alvorlige hendelsene kjent at også lokomotivføreren i flytog 3816 søndag 17. april kl. 0112 meldte fra til togleder om tilsvarende signalobservasjon med forsignalet på signal N 4323 på Sandvika stasjon. Havarikommisjonen ble ikke varslet om denne hendelsen. Det er viktig å påpeke at slike alvorlige hendelser umiddelbart må rapporteres videre i Jernbaneverkets interne system, for å sikre at lignende problemer blir håndtert på et langt tidligere tidspunkt.

2.2 Årsaksfaktorer relatert til sikkerhetsstyring og ledelse

2.2.1 Spesifikasjoner

Spesifikasjonene som var vedlegg til kontrakten var på norsk. Disse ble oversatt til engelsk, og tolket av leverandøren som benyttet tysk som arbeidsspråk. Avklaringer fra Jernbaneverket ble også oversendt på norsk til Leverandøren. Basis for utvikling av grensesnittet mot relélinjeblokk i GMB-prosjektet bestod i hovedsak av reléskjemaer.

Det er lite sannsynlig at uklarheter rundt spesifikasjonen har vært årsak til at feilen har oppstått, men det er sannsynlig at man med en mer formell og analytisk prosess rundt gransking av leverandørens designdokumenter kunne ha avdekket mangler i designet.

Det er lite sannsynlig at en bedre prosess rundt oversettelse av norsk kravspesifikasjon til engelsk kunne ha hindret at den aktuelle feilen i programvaren oppstod. Dette fordi feilsituasjonen er basert på svært detaljerte systemforutsetninger som ikke var med i den opprinnelige kravspesifikasjonen. Det er derfor heller ikke sannsynlig at feilsituasjonen har oppstått på grunn av svakheter i selve kravspesifikasjonen, siden den oppstod som en følge av forhold som er systemspesifikke og ikke naturlig hører hjemme i en funksjonsorientert kravspesifikasjon.

Det er ingen ting som tyder på at mangelfulle spesifikasjoner for linjeblokkfunksjonen har vært årsak til at feilen oppstod. Uten leverandørens kunnskap og erfaring på dette området, samt kundens involvering, kunne dette blitt et problemområde i utviklingsprosessen og skapt forsinkelser i prosjektet.

2.2.2 RAMS-prosess

SIMIS-C er et velprøvd sikringsanlegg som er utviklet før EN 50126, -128 og -129 standardenes tid. Tilpasning av SIMIS-C for Gardermobanen skulle, i henhold til kontrakten mellom Siemens og Gardermobanen, skje i henhold til EN 50126, -128 og -129 standardene.

For programvareutviklingen er det dokumentert at EN50128 på de fleste områdene er fulgt. Dette er gjort ved å kryssjekke og dokumentere at krav i EN 50128 er ivaretatt med den prosessen Siemens har fulgt (basert på MÜ8004). Det er brukt metoder som svarer til ”HR” (Highly Recommended) -kravene i standarden. Dette er synliggjort i dokumentasjonen både ved utvikling og ved valideringen av systemet.

Dette ble funnet tilstrekkelig både av Siemens interne og uavhengige valideringsenhet (Prüfleistelle) og assessor.

Dokumentasjonen som er gjennomgått i forbindelse med denne analysen og som beskriver de metoder som leverandøren har benyttet ved utvikling og test av programvaren, tilsier at man burde ha oppdaget feilen. Det synes imidlertid klart at den kombinasjonen av inngangsvariabler og feiltilstander, som førte til situasjonen på Slependen, ikke ble identifisert verken i utviklings- eller valideringsprosessen. Dette bekreftes også av leverandøren selv i forbindelse med egen gransking av hendelsen.

Spørsmålet er om en, til tross for at en i utgangspunktet kan godtgjøre at en følger EN 50128, likevel ikke har gode nok metoder til å hindre denne type feil.

Feilen som oppstod var basert på at flere hendelser inntraff i en bestemt rekkefølge. For å kunne se for seg, og hindre at denne type feil kan oppstå, må man ved hjelp av systematisk metodikk identifisere alle tenkte tilstander og feilmodi et system, delsystem eller modul kan innta. Det er her EN-standardene skal bidra til at man ved en systematisk gjennomgang av tenkelige hasarder i en tidlig fase i utviklingen kan identifisere muligheter for denne type feil, og dermed få et større fokus på dette både under utvikling og validering.

For å få til en fullgod analyse som beskrevet ovenfor er det en rekke forhold som må være kjent:

- Systemets, delsystemets eller modulens egenskaper og virkemåte
- Tilstøtende systemers egenskaper og virkemåte
- Drifts- og vedlikeholdsrutiner
- Eksterne påvirkninger

Utfordringen i denne typen analyser er å sette sammen en gruppe personer som innehar god nok kompetanse på alle disse forholdene. Dette kan være en spesiell utfordring for systemleverandøren når en skal tilpasse et system til en ny og ukjent infrastrukturforvaltning.

I GMB-prosjektet innså en etter hvert at prosjektet og Siemens måtte jobbe sammen for å oppnå riktig funksjonalitet. Denne måten å arbeide på ble i hovedsak brukt til å gjennomgå avklaringer og få riktig funksjonalitet, og ikke til å identifisere feilmodi og feiltilstander for systemet og dets grensesnitt.

De tre hasardanalysene som ble utarbeidet var på et overordnet nivå og ikke egnet til å fange opp kombinasjoner av feil og feilmodi inne i de ulike programvaremodulene eller i grensesnittet mellom modulene. Disse analysene ble også for en stor del utført etter at utvikling og validering var gjennomført. Dette var ikke er i henhold til EN 50126's intensjon.

Ut i fra de undersøkelser som er foretatt er følgende avdekket:

- det ble ikke gjort en hasardidentifisering tidlig i prosjektet (fase 3 i livssyklusmodellen i EN 50126)
- det forelå ingen hasardanalyse fra oppdragsgiver (Gardermobanen) (fase 1 og 2 i livssyklusmodellen i EN 50126) som underlag for leverandørens analyse
- det ble ikke fokusert spesielt på grensesnitt

Det er derfor grunnlag for å si at EN50126 ikke er fulgt helt ut for tilpasningen av SIMIS-C, og at dette kan ha medvirket til at feilen som ble liggende i det generiske systemet ikke ble oppdaget.

Det ble heller ikke gjennomført automatiserte tester av programvaren. Ved bruk av slike tester vil man i større grad kunne øke testomfanget og teste kombinasjoner som ikke er praktisk mulig med manuelle tester. Ved utstrakt bruk av automatiserte tester av programvaren, ville feil av typen som ble identifisert i SIMIS-C -anlegget med stor sannsynlighet blitt oppdaget under testing.

Med en full implementering av EN 50126, -128 og -129 standardene i utviklingsprosessen hadde man trolig hatt større mulighet for å finne feilen som ble liggende i det generiske systemet i SIMIS-C. Dette tilskrives først og fremst at man ville gjennomført en grundigere hasardanalyse i forkant av utviklingen, samt hatt et større fokus på grensesnitt.

Det må imidlertid presiseres at EN-standardene var i tidlige - og foreløpige versjoner, og at det ikke fantes noen vesentlig erfaring med bruk av standardene noe sted i Europa på den tiden. Det er derfor grunn til å anta at effekten av en raskere implementering av standardene i Siemens samlet sett ikke nødvendigvis ville ha bidradd positivt i forhold til den etablerte og velkjente sikkerhetsprosessen de hadde.

2.3 Årsaksfaktorer relatert til driftstillatelse og myndighetsgodkjenning

Årsaksforhold relatert til driftstillatelse og myndighetsgodkjenning omhandler kun Jernbaneverkets interne typegodkjenning.

2.3.1 Prosjektering og bygging av nytt sikringsanlegg på Sandvika stasjon

Den generiske delen av SIMIS-C (hvor feilen ble funnet) ble ansett som validert og godkjent, og derfor ble ikke denne delen validert spesielt i forbindelse med SIMIS-C på Sandvika stasjon.

Sikkerhetsprosessen som ble valgt i Sandvika–Asker -prosjektet bygger på aksepterte prinsipper om at den generiske delen av et system som er godkjent tidligere ikke skal måtte valideres og verifiseres på nytt for å bli godkjent. Dette er et prinsipp som EN 50126, -128 og -129 standardene også legger opp til. Testing og godkjenning vil da basere seg på den anleggsspesifikke delen. Det generiske systemet ansees som godkjent på basis av tilhørende generisk sikkerhetsdokumentasjon (Generic Product Safety Case).

Man kan stille spørsmål om det burde ha vært gjennomført en ny validering av det generiske systemet i forbindelse med Sandvika på bakgrunn av at det ikke var fulgt en prosess i henhold til EN 50126, -128 og -129 standardene fullt ut på Gardermoen, samt at systemet ikke var endelig typegodkjent av Jernbaneverket. Det finnes derimot en del argumenter som tilsier at dette ikke skulle være nødvendig:

- man hadde en drifts-/erfaringstid på systemet på 6-7 år på Gardermobanen
- systemet hadde i lengre tid vært i bruk i andre forvaltninger (blant annet hos VR i Finland).
- det var kun formaliteter som hindret at en endelig godkjenning fra Jernbaneverket forelå tidligere.

3. KONKLUSJON

Feilen som var årsaken til de alvorlige hendelsene var relatert til det generiske systemet som ble utviklet og validert i forbindelse med implementering av SIMIS-C på Gardermobanen. Feilen oppstod ikke som en følge av implementering av SIMIS-C på Sandvika stasjon. I henhold til etablerte prinsipper, som er i tråd med EN 50126, -128 og -129 standardene, skal det ikke være nødvendig å validere et generisk system som er godkjent fra før. En kan derfor konkludere med at det ikke kan forventes at den type feil som fantes i det generiske systemet burde vært oppdaget ved implementering av SIMIS-C på Sandvika stasjon.

På basis av de undersøkelser som er gjort kan det ikke dokumenteres at prosessen i EN50126 er fulgt fullt ut ved tilpasning av SIMIS-C til Gardermobanen. Det ble ikke gjennomført nødvendig hasardidentifisering og analyser under de tidlige fasene slik EN 50126 krever. Dette kan ha vært en indirekte årsak til at feilen i generisk programvare ikke ble oppdaget i utviklings- og valideringsprosessen, til tross for at en fulgte MÜ8004 som i hovedsak tilfredsstiller kravene i EN 50128.

Ser en på den tekniske feilen som oppstod er feilhendelsene; filamentfeil, elementsperre og omstart av BSTR alle normale hendelser som kan opptre med en viss frekvens. Det at en på bakgrunn av disse hendelsene, selv om de må opptre i en bestemt rekkefølge, kan få den type feil som her oppstod, bør være mulig å identifisere for deretter å innføre tiltak for å hindre at det kan skje. Baserer en det meste av valideringen på tester er det nesten umulig å definere alle tenkelige tester for å kunne avdekke en slik feil uten at en på forhånd har hatt en analytisk tilnærming med hasardidentifisering og analyse. Spesielt viktig er dette for å få en nødvendig oversikt over det totale systemet inkludert eksterne grensesnitt, driftsformer og andre påvirkninger utenfor selve systemet. Dersom det er vanskelig å analysere ulike sammenhenger og kombinasjoner bør man benytte testmetoder (automatiserte) som kan kompensere for dette.

3.1.1 Manglende oversikt over dokumentasjon.

Ved forespørsel om dokumentasjon viste det seg at det var vanskelig å finne de generiske dokumentene som tilhører anleggene på Sandvika – Asker og Gardermobanen. Det kan synes som om dokumentene ikke er hensiktmessig arkivert i forhold til at de tilhører et generisk produkt som man benytter i flere anlegg. Som eksempel på manglende dokumentoversikt kan nevnes at man for å få tak i sikkerhetsdokumentasjon for Gardermobanen søkte i dokumentdatabasen med fritekst. Resultatet av dette søket virket noe tilfeldig og uoversiktlig. Et annet eksempel er assessorrapporten for Gardermobanen som man var nødt til å gå til Sintef for å skaffe.

3.1.2 Overlevering fra utbyggingsprosjekt til drift.

Ved gjennomgang av dokumentasjon for Gardermobanen var det vanskelig å identifisere hvilke dokumenter og hvilke anvendelsesbetingelser som overføres fra utbyggingsprosjektet til drift. Viktige forhold og anvendelsesbetingelser kan lett forsvinne i den store dokumentasjonsmengden som et slikt prosjekt genererer.

3.1.3 Endring av testprosedyrer

Havarikommisjonen er kjent med at leverandøren har gjort endringer i testprosedyrene for testing av grensesnitt.

3.1.4 Driftsforhold

Når alvorlige signalhendelser blir meldt, er det viktig at dette umiddelbart blir håndtert på en sikkerhetsmessig betryggende måte slik at farlige situasjoner avverges.

3.1.5 Øvrige iakttakelser

Det ble observert umotivert blinkende lysdioder på grensesnittet mot Slependen blokkpost. Ved hjelp av målinger ble det konstatert at det var varierende støy på grensesnittet. Dette kan ha hatt sammenheng med de hyppige feil (elementsperrer) som hadde oppstått. Grensesnittet er ømfintlig for støy, og det er derfor viktig at kabler som blir benyttet til dataoverføring mot dette grensesnittet har god standard, slik at driftsfeil unngås. Løse måleledninger og provisoriske koblinger på Slependen blokkpost og i relérommet på Sandvika stasjon etterlot et inntrykk av at det var en situasjon ved stillverket som var under observasjon og forberedelse for utbedring.

Havarikommisjonen er av den oppfatning at Siemens har tatt tak i problemet på en bra måte, og gjort en grundig jobb i å finne feilen og årsaken til denne, samt vært åpne og behjelpelige under prosessen.

4. SIKKERHETSTILRÅDINGER

Undersøkelsen av denne jernbaneulykken/alvorlige jernbanehendelsen har avdekket flere områder hvor havarikommisjonen anser det nødvendig å fremme sikkerhetstilrådinger som har til formål å forbedre jernbanesikkerheten.

Undersøkelsesrapporten oversendes Samferdselsdepartementet som treffer nødvendige tiltak for å sikre at det tas behørig hensyn til sikkerhetstilrådingene, jf. forskrift 31. mars 2006 nr. 378 om offentlige undersøkelser av jernbaneulykker og alvorlige jernbanehendelser m.m. (jernbaneundersøkelsesforskriften) § 16.

Det ble ikke fremmet umiddelbare sikkerhetstilrådinger som et resultat av disse hendelsene. Havarikommisjonen registrerte at leverandøren av sikringsanlegget raskt anbefalte Jernbaneverket å ta alle grensesnitt, som var av samme konstruksjon, ut av drift på de øvrige strekningene med samme type sikringsanlegg. Alle tilsvarende grensesnitt ble derfor satt ut av drift inntil feilen var rettet og ny driftsprøve var utført.

Sikkerhetstilråding JB nr. 2007/02

Havarikommisjonen tilrår Statens Jernbanetilsyn å vurdere å anbefale Jernbaneverket å gjennomgå sin RAMS prosess i henhold til EN 50126 for alle ledd og faser for tilsvarende prosjekter, både i egen organisasjon og hos sine underleverandører for å sikre best mulig etterlevelse av standarden og dens intensjoner. Det bør skapes en forståelse for hvorfor dette er viktig.

Sikkerhetstilråding JB nr. 2007/03

Hver gang det skal implementeres et nytt sikringsanlegg oppstår en sikkerhetsmessig utfordring i forhold til grensesnitt mot eksisterende sikringsanlegg, det være seg reléanlegg eller elektroniske anlegg.

Havarikommisjonen tilrår Statens Jernbanetilsyn å vurdere å anbefale Jernbaneverket å fokusere spesielt på grensesnitt, både systemmessig og driftsmessig ved implementering av nye sikringsanlegg.

Sikkerhetstilråding JB nr. 2007/04

Togledelsen iverksatte ikke umiddelbare tiltak etter den første hendelsen. Det er viktig å påpeke at slike alvorlige hendelser blir ivaretatt og rapportert videre i Jernbaneverkets interne system, slik at lignende forhold blir håndtert på et langt tidligere tidspunkt.

Havarikommisjonen tilrår Statens Jernbanetilsyn å vurdere å anbefale Jernbaneverket å gjennomgå prosedyre for håndtering av innmeldte signalfeil til togledelsen, for å se om denne er hensiktsmessig.

Tilrådinger i forhold til øvrige observasjoner:

Havarikommisjonen er kjent med at forholdene nevnt i sikkerhetstilrådingene i pkt. 4.4 og 4.5 skal ivaretas av sikkerhetsforskriftens krav til teknisk dokumentasjon og til sikkerhetsoppfølgingsplan. Havarikommisjonen velger allikevel, på bakgrunn av hendelsens store potensial, å fremme disse forholdene til vurdering.

Sikkerhetstilråding JB nr. 2007/05

Havarikommisjonen tilrår Statens Jernbanetilsyn å vurdere å anbefale Jernbaneverket å utarbeide en hensiktsmessig måte å lagre generisk systemdokumentasjon, inklusive sikkerhetsdokumentasjon, slik at dette strukturmessig henger sammen, og at man til enhver tid lett kan finne gyldig versjon av dokumentene for alle Jernbaneverkets system og anlegg.

Sikkerhetstilråding JB nr. 2007/06

Havarikommisjonen tilrår Statens Jernbanetilsyn å vurdere å anbefale Jernbaneverket at de ved overlevering av anlegg fra utbyggingsprosjekt til drift har et større fokus på å identifisere hvilken dokumentasjon som ligger til grunn for drift og vedlikehold av anlegget, samt at man har et system for å videreføre og følge opp anvendelsesbetingelser. Spesielt viktig er dette for RAMS-relaterte anvendelsesbetingelser.

BILAG

Ingen

5. VEDLEGG

1. Oversikt over aktuelle dokumenter som har relevans for feilen, og som er benyttet som grunnlagsmateriale for rapporten

Statens Havarikommisjon for Transport
Lillestrøm, 20. februar 2007