Retteinstruks Eksamen INF5150 Høsten 2004

UNIVERSITETET I OSLO

Det matematisk-naturvitenskapelige fakultet

Eksamen i:	**INF 5150**	**Uangripelige IT-systemer**
Eksamensdag:	**6. desember 2004**	
Tid for eksamen:	**09.00 – 12.00**	
Oppgavesettet er på … side(r)	**2**	
Vedlegg:	**0**	
Tillatte hjelpemidler:	**Alle skriftlige dokumenter kan benyttes**	

Kontroller at oppgavesettet er komplett
før du begynner å besvare spørsmålene.

Flere tannleger i et tannlegesenter

Denne oppgaven bygger på obligen der en tannlege benytter SMS til innkalling, påminnelse og bestilling av timer.

Systemet skal nå ikke bare gjelde for én tannlege, men for et tannlegesenter med flere tannleger som deler pasientene.

1. Hver pasient tilordnes en tannlege som ”fasttannlege”
2. Ved normal innkalling skal pasienten få time hos sin fasttannlege. Pasienten skal bekrefte at den gitte timen passer, eller be om en ny time.
3. Hvis en tannlege er syk, vil de andre tannlegene overta pasientene til denne tannlegen. De vil da sende ut SMS hvor de innkalte pasienter kan velge om de vil ha ny time eller om de vil behandles av en annen enn sin fasttannlege. De pasientene som ikke svarer innen en gitt tid, antas å ville behandles av en vikar. (Tips: Definer en timer som en egen lifeline.)

Del 1 Oppgave 1 Modellering (35%)

Vår tannlege skal inngå i et samarbeid i et tannlegesenter. De bestiller et system som skal kunne tilfredsstille spesifikasjonen over. Du skal bidra til å spesifisere dette systemet ved

å modellere det i UML 2.0. Du må i alle fall beskrive systemet med de følgende elementene:

a. (5%) Et klassediagram som viser de mest sentrale begrepene. Ett av disse begrepene er 'Pasient' som representerer informasjon om klienten i systemet og som skal ha en avtale som et attributt.
b. (10%) Et eller flere composite structure diagrammer som viser systemets arkitektur og kommunikasjonsveier.
c. (10%) Ett eller flere sekvensdiagrammer som baserer seg på den composite structure som ble beskrevet i oppgave 1b, og som beskriver oppførselen av systemet i henhold til punktene 1,2,3 over. Lag ett oversiktsdiagram (gjerne et Interaction Overview Diagram) som viser hvordan de enkelte sekvensdiagrammer henger sammen.
d. (10%) Ett eller flere tilstandsdiagrammer (State Machines) som beskriver de deler som er viktigst for oppførselen. Hvilken eller hvilke tilstandsmaskiner som skal beskrives er avhengig av hvilken arkitektur du har valgt under b, men 'Pasient' skal beskrives som en av tilstandsmaskinene.

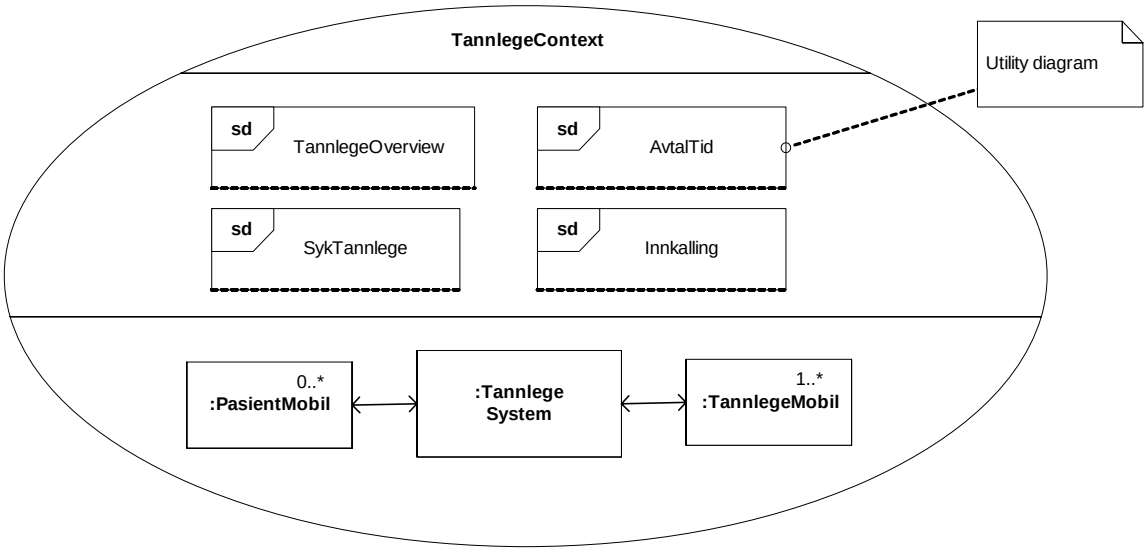
Retteinstruks Oppgave 1 Modellering

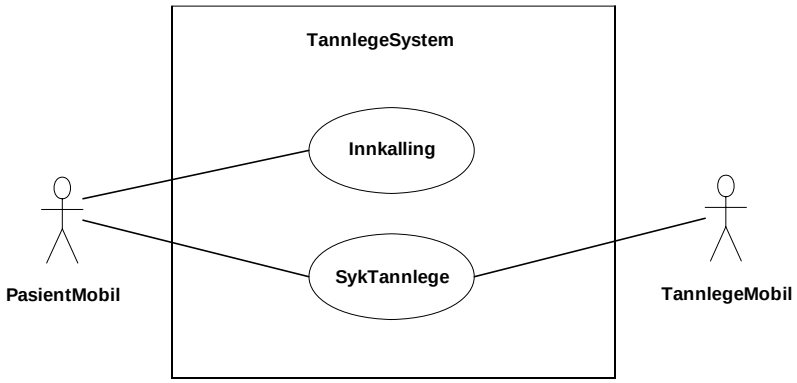
I år er oppgaven ganske åpen – kanskje for åpen. Det vil kunne gi grobunn for løsninger der man har lagt for mye i data og i ymse finurlige operasjoner på objektene. Det følgende er hva jeg tenkte meg var "opplagt" da jeg lagde oppgaven, men det er klart at det neppe var opplagt. Å lage en detaljert fasit langs disse linjene blir kanskje litt meningsløst fordi man må vurdere kandidatens løsning og ikke kun om vedkommende har tenkt som meg.

a. Klassediagrammet bør inneholde Pasient og Tannlege og de kan godt ha felles abstrakt superklasse – f.eks. Person. Pasienten bør vite om sin fasttannlege og sin avtale. Pasienten behøver ikke kunne ha mer enn 1 avtale av gangen. 'Avtale' er altså også et viktig begrep. Tannlegen kjenner alle sine pasienter som har avtale, og tannlegen kjenner alle sine pasienter som han er fasttannlege for. Tannlegen har kanskje også en peker til sin vikar. Det kan også være aktuelt med noen begreper som betegner begreper i systemets omgivelser som f.eks. pasienters mobiltelefoner.
b. Composite structure diagrammet må ha et sett av Pasienter. Helst bør det være et sett av Tannleger også som kommuniserer med settet av pasienter. Mange vil også ha en kontroller som en styreprosess i strukturen, men det er strengt tatt ikke helt nødvendig. Routing kan evt. skje i portene. Jeg setter pris på at kandidatene har strødd porter rundt omkring i forbindelse med konnektorene.
c. Sekvensdiagrammene skal være basert på composite structure fra b. Hvis det er med elementer som ikke er i strukturen, så er det klart trekk. Det er ikke nødvendig å vise høyere nivå enn Tannlegesystemet, men om det gjøres, så skal selvfølgelig decomposition være riktig utført. Handlingen må selvfølgelig grovt sett følge beskrivelsen i prosa gitt i begynnelsen av oppgaven. Det er naturlig både å vise Innkalling og SykTannlege.
d. Etter min modell ville Pasient og Tannlege være klare kandidater. Andre vil la

Kontroller være helt sentralt. Pasient må være med. Det er intet absolutt krav til hvordan tilstandsrommet skal være, men jeg setter pris på at det er mer enn 1 tilstand fordi pasienten jo gjerne er i ulike tilstander. Under innkalling har vi tilstander knyttet til respons og det gjelder også ved kommunikasjonen om syk fasttannlege. Flere tilstander er i denne sammenheng bedre enn bare 1 tilstand selvom man kan skille på signalene som sendes.

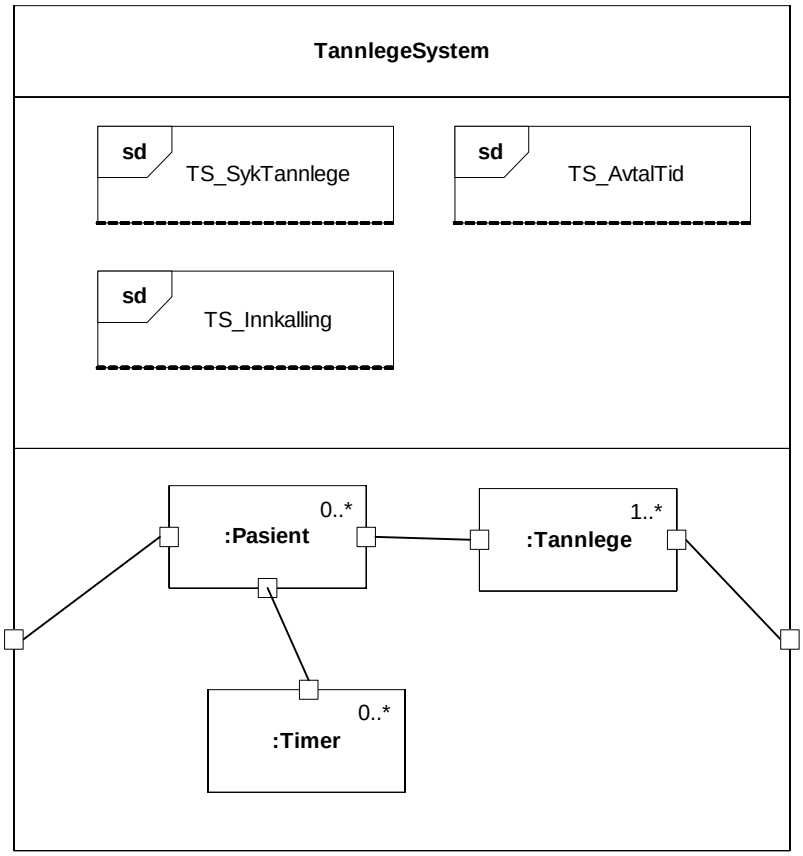
Kontekst og use case[1]



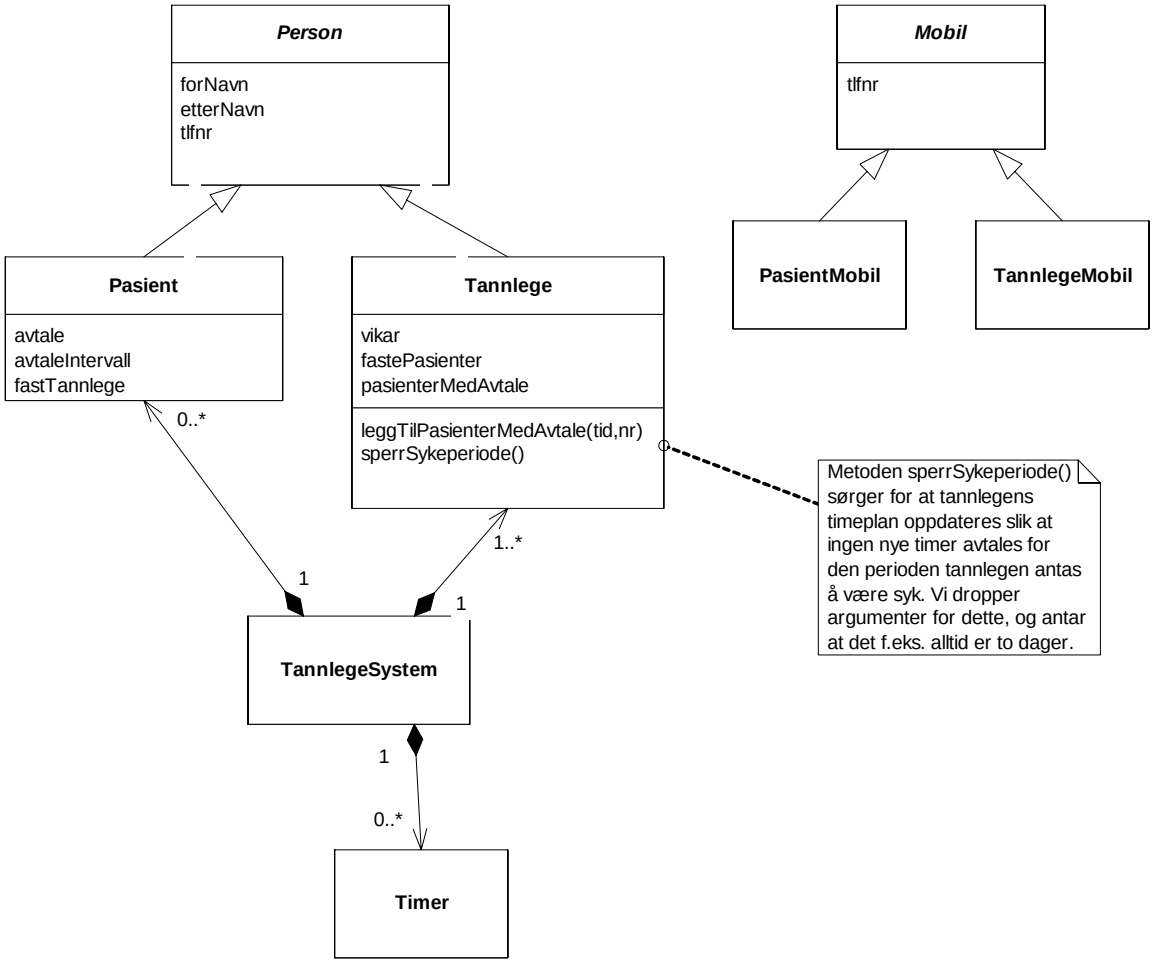


[1]Øystein har følgende kommentarer til Atle Refsdals diagrammer:
1. Jeg tror ikke oppgaven krevde at man gav kontekstdiagrammet, men det gjør ikke annen skade enn at du behøver å gjøre dekomponering som selvfølgelig blir litt dobbelt opp.
2. I InteractionOverview diagrammet tror jeg at man bør ha en diamant også som merge-node før final-node. (ikke viktig for studentene synes jeg)
3. Jeg hadde foretrukket at du hadde vist 2 pasienter p[u] og p[v]. Det hadde kunnet indikere at det er en multicast involvert ved syk tannlege (der alle pasientene til den syke tannlegen skal varsles). Formelt sett blir jo da model-checkinga et lite hakk mer komplisert, men det tenkte jeg faktisk ikke på.

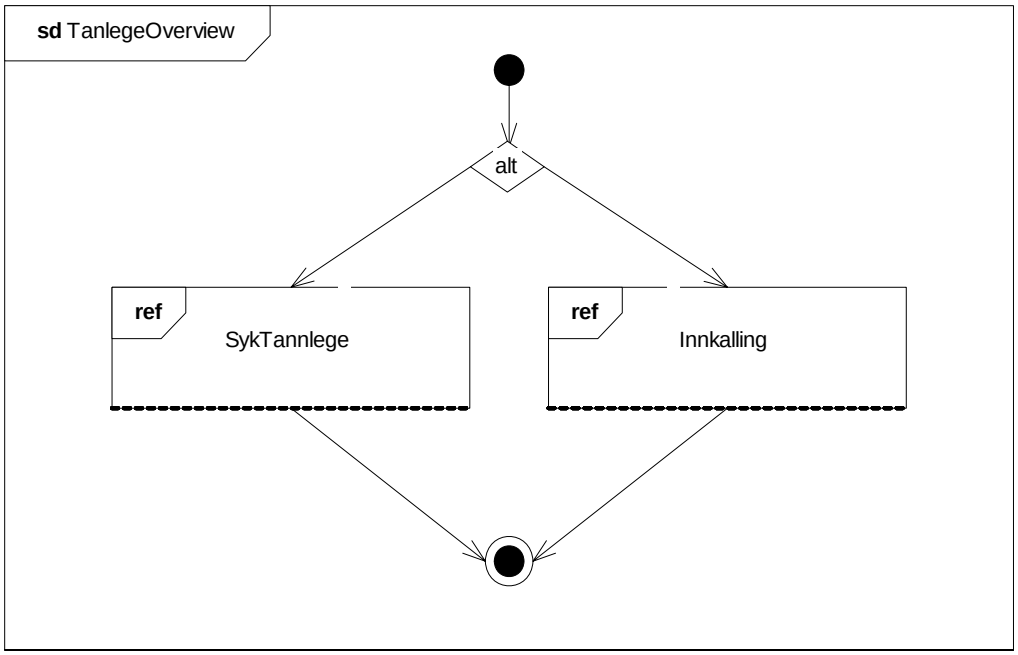
Struktur


TannlegeSystem
sd
TS_SykTannlege
sd
TS_AvtalTid
sd
TS_Innkalling
0..*
:Pasient
1..*
:Tannlege
0..*
:Timer

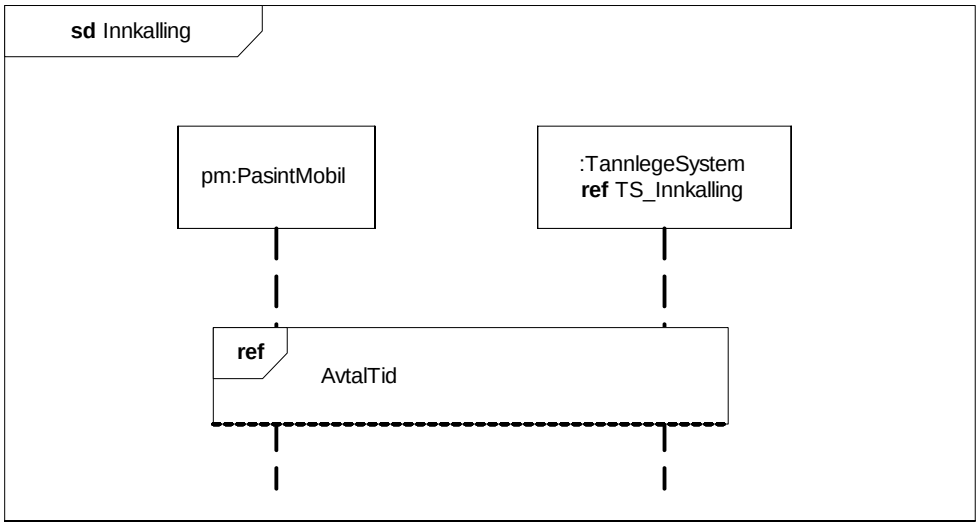
Klasser

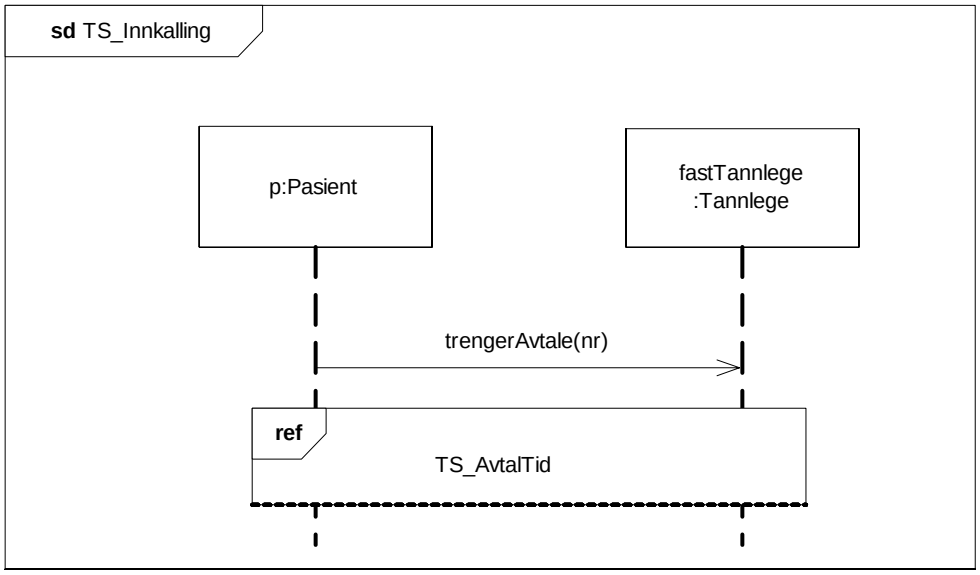

Person
forNavn
etterNavn
tlfnr
Mobil
tlfnr
Pasient
avtale
avtaleIntervall
fastTannlege
Tannlege
vikar
fastePasienter
pasienterMedAvtale
leggTilPasienterMedAvtale(tid,nr)
sperrSykeperiode()
PasientMobil
TannlegeMobil
0..*
1..*
1
1
TannlegeSystem
1
0..*
Timer
Metoden sperrSykeperiode() sørger for at tannlegens timeplan oppdateres slik at ingen nye timer avtales for den perioden tannlegen antas å være syk. Vi dropper argumenter for dette, og antar at det f.eks. alltid er to dager.

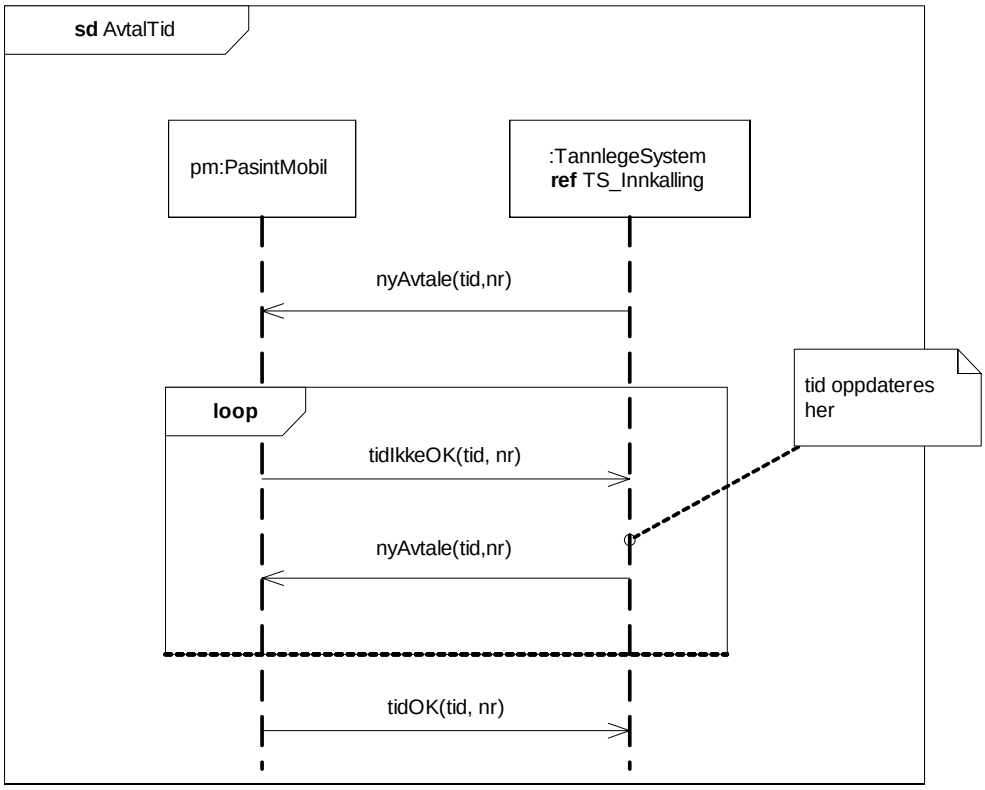
Overview

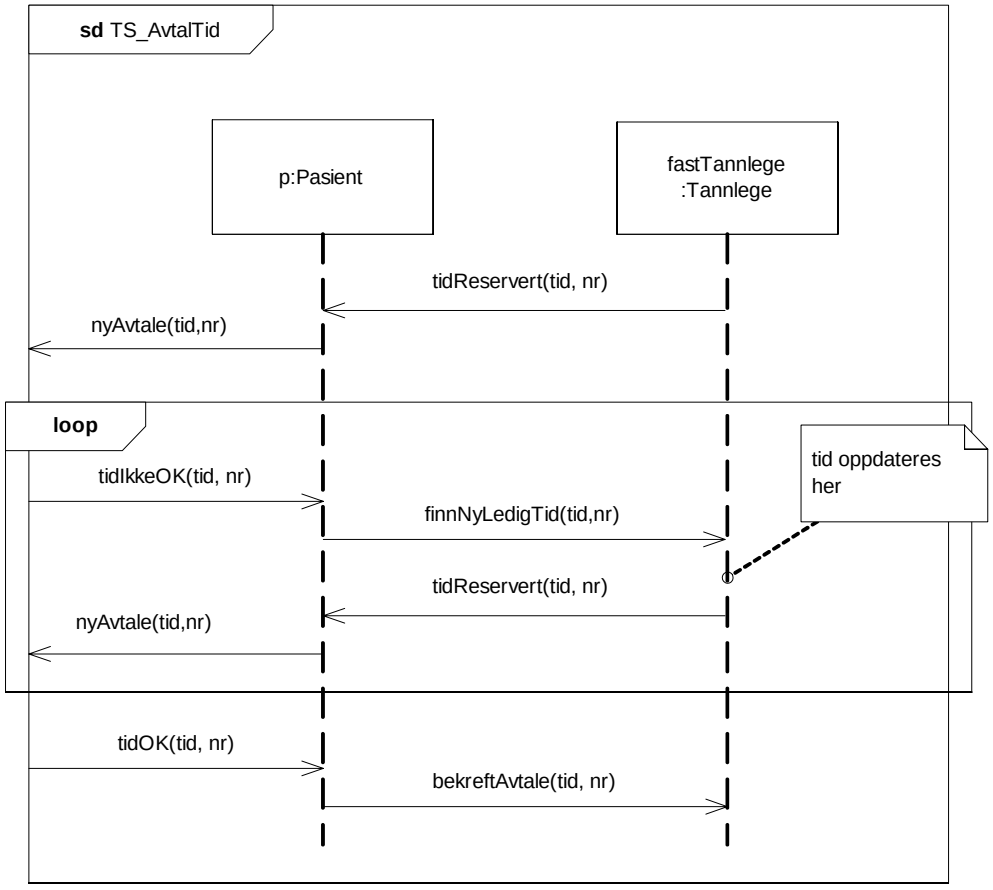


Innkalling

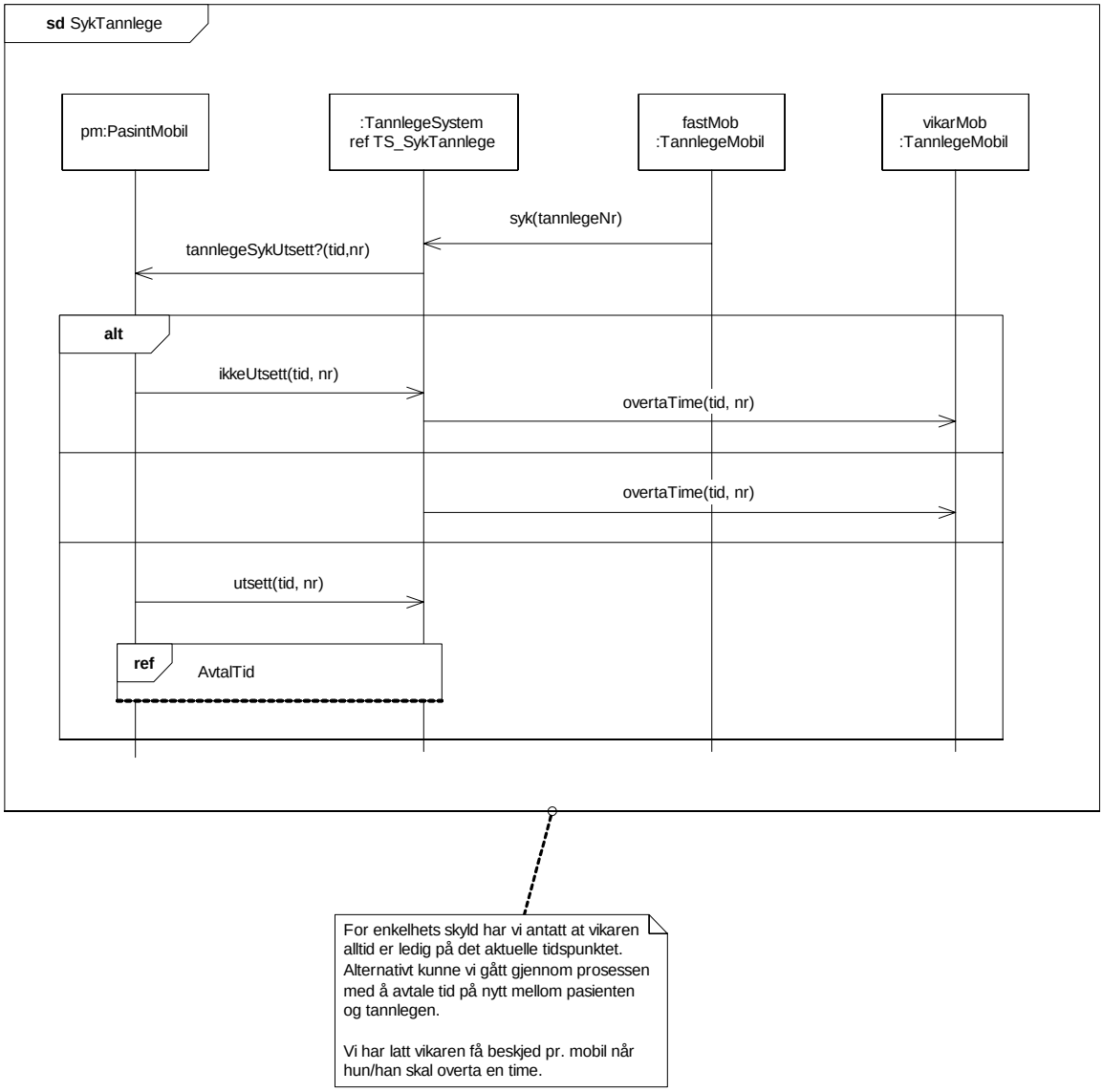

sd Innkalling
pm:PasintMobil
:TannlegeSystem
ref TS_Innkalling
ref
AvtalTid

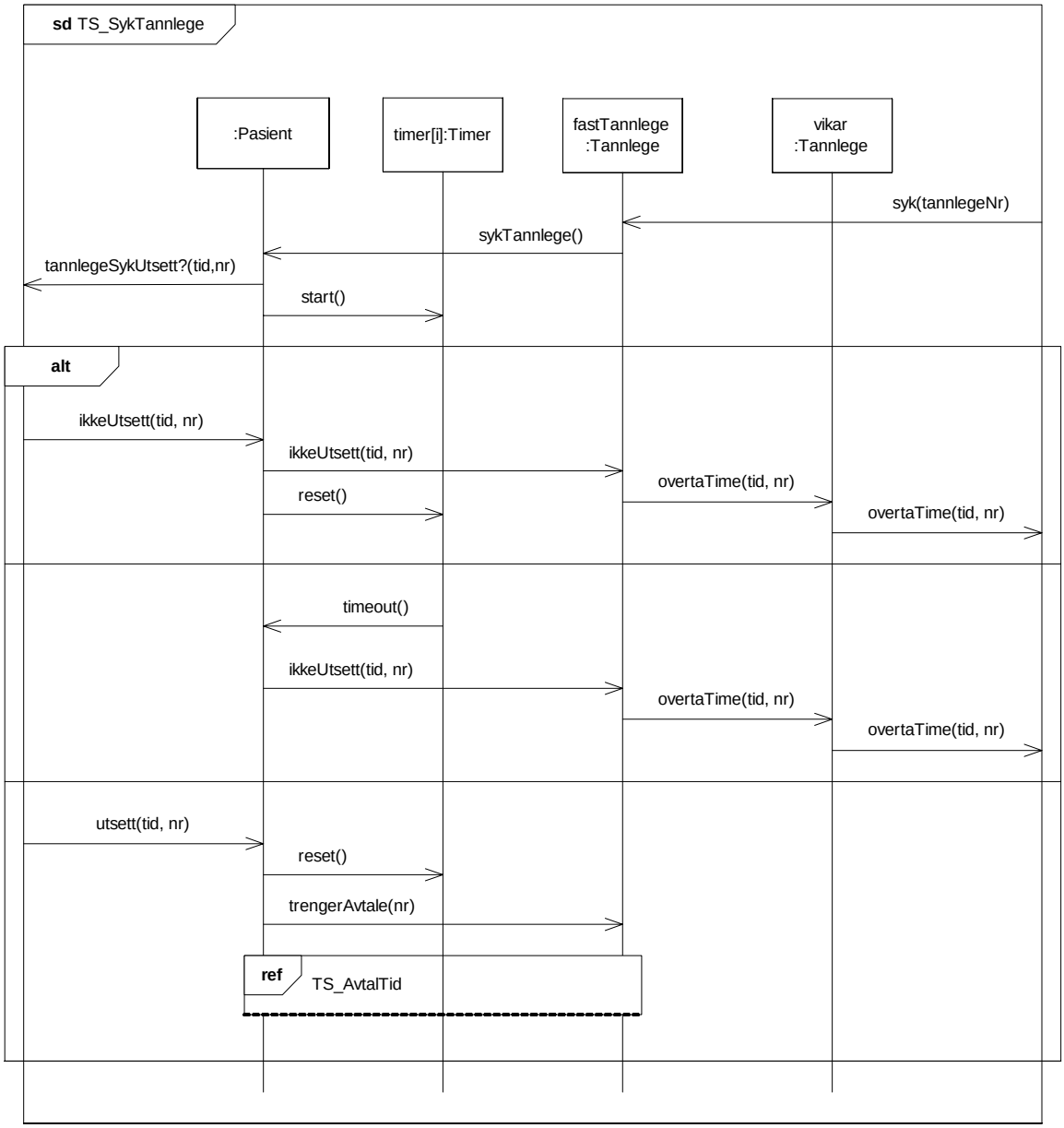

sd TS_Innkalling
p:Pasient
fastTannlege
:Tannlege
trengerAvtale(nr)
ref
TS_AvtalTid


sd AvtalTid
pm:PasintMobil
:TannlegeSystem
ref TS_Innkalling
nyAvtale(tid,nr)
loop
tid oppdateres her
tidIkkeOK(tid, nr)
nyAvtale(tid,nr)
tidOK(tid, nr)

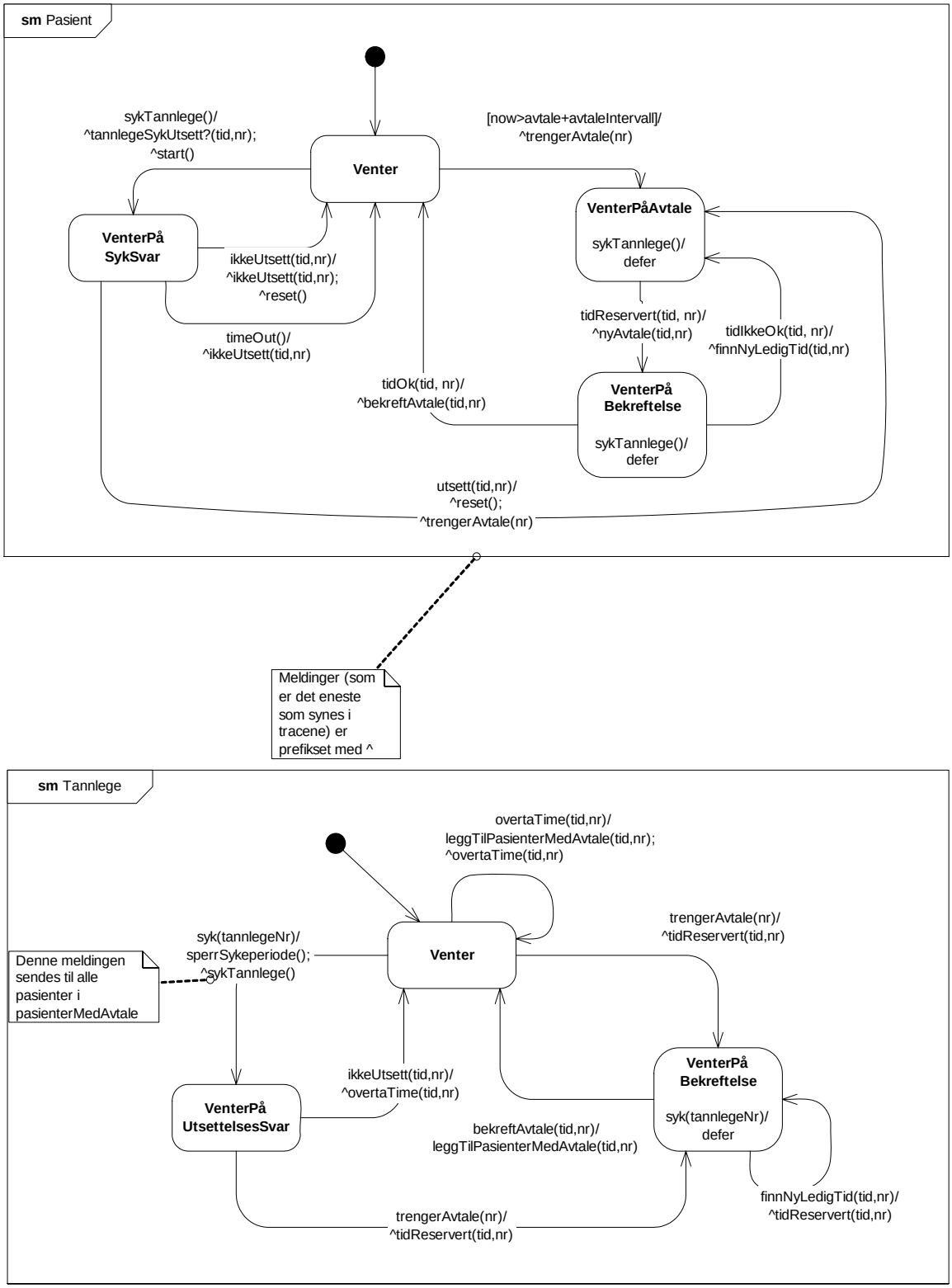

sd TS_AvtalTid
p:Pasient
fastTannlege
:Tannlege
tidReservert(tid, nr)
nyAvtale(tid,nr)
loop
tid oppdateres her
tidIkkeOK(tid, nr)
finnNyLedigTid(tid,nr)
tidReservert(tid, nr)
nyAvtale(tid,nr)
tidOK(tid, nr)
bekreftAvtale(tid, nr)

Syk tannlege




sd TS_SykTannlege
:Pasient
timer[i]:Timer
fastTannlege :Tannlege
vikar :Tannlege
syk(tannlegeNr)
sykTannlege()
tannlegeSykUtsett?(tid,nr)
start()
alt
ikkeUtsett(tid, nr)
ikkeUtsett(tid, nr)
overtaTime(tid, nr)
reset()
overtaTime(tid, nr)
timeout()
ikkeUtsett(tid, nr)
overtaTime(tid, nr)
overtaTime(tid, nr)
utsett(tid, nr)
reset()
trengerAvtale(nr)
ref
TS_AvtalTid

Tilstandsmaskiner



Oppgave 2 Verifikasjon (30%)

I denne oppgaven skal du overbevise oss om at systemet du har spesifisert er konsistent.

a. (10%) Beskriv i detalj fem forskjellige tracer av sekvensdiagrammene du lagde i oppgave 1c
b. (10%) Påvis ved en partiell simulering av tilstandsmaskinen for Pasient som du lagde i oppgave 1d at den tilfredsstiller spesifikasjonene i oppgave 1c
c. (10%) Drøft hva du nå har vist om systemet gjennom å løse oppgave 2b. Forklar hvordan systemet av tilstandsmaskiner forholder seg til spesifikasjonen av sekvensdiagrammer i oppgave 1c. Vurder supplering, innsnevring, detaljering, raffinering eller andre relevante begreper du har lært i kurset Begrunn svaret med referanse til definisjonene.

Retteinstruks Oppgave 2 Verifikasjon

Oppgave 2 er jo avhengig av den åpne oppgaven 1 og må derfor sees i lys av kandidatens løsning av den.

a. Sjekk at tracene faktisk er tracer i kandidatens sekvensdiagrammer.
b. Under dette punktet bør sensor legge vekt på forklaringen av sammenhengen mellom sekvensdiagram og tilstandsmaskin. Det essentielle ved den partielle simuleringen er at man tar utgangspunkt i sekvensdiagrammet og traverserer i prinsippet alle sekvenser i det. For hver trace sjekker man at Pasient tilstandsmaskinen oppfører seg som sekvensdiagrammets lifeline(s) for Pasient(er). Aller først skal kandidaten påpeke at sekvensdiagram og tilstandsmaskin må alignes. Deretter antas at sekvensdiagrammet gjelder til det kommer en input til Pasient-tilstandsmaskinen. Da utføres tilstandsmaskinens transisjon og man sjekker at effekten er beskrevet korrekt i sekvensdiagrammet. Så går man tilbake til sekvensdiagrammet etc.
c. I prinsippet er 2c uavhengig av hva kandidaten har gjort på opg1 og opg2a+b. Kandidaten bør konkludere med at systemet av tilstandsmaskiner vil kunne framvise et sett av sekvenser som er en supplering av spesifikasjonen av sekvensdiagrammer fra 1c. For å få full pott må kandidaten ha vist overbevisende til litt raffineringsdefinisjoner gitt ved matematikk eller i alle fall referert overbevisende til disse definisjonene.

2 a.
Tracene t1-t3 er beskrevet av diagrammene Innkalling og TS_Innkalling:

t1=
<!trengerAvtale(nr)
?trengerAvtale(nr)
!tidReservert(tid,nr)
?tidReservert(tid,nr)
!nyAvtale(tid,nr)
?nyAvtale(tid,nr)

!tidOK(tid,nr)
?tidOK(tid,nr)
!bekreftAvtale(tid,nr)
?bekreftAvtale(tid,nr)>

t2=
<!trengerAvtale(nr)
?trengerAvtale(nr)
!tidReservert(tid,nr)
?tidReservert(tid,nr)
!nyAvtale(tid,nr)
?nyAvtale(tid,nr)
!tidIkkeOK(tid,nr)
?tidIkkeOK(tid,nr)
!finnNyLedigTid(tid,nr)
?finnNyLedigTid(tid,nr)
!tidReservert(tid,nr)
?tidReservert(tid,nr)
!nyAvtale(tid,nr)
?nyAvtale(tid,nr)
!tidOK(tid,nr)
?tidOK(tid,nr)
!bekreftAvtale(tid,nr)
?bekreftAvtale(tid,nr)>

t3=
<!trengerAvtale(nr)
?trengerAvtale(nr)
!tidReservert(tid,nr)
?tidReservert(tid,nr)
!nyAvtale(tid,nr)
?nyAvtale(tid,nr)
!tidIkkeOK(tid,nr)
?tidIkkeOK(tid,nr)
!finnNyLedigTid(tid,nr)
?finnNyLedigTid(tid,nr)
!tidReservert(tid,nr)
?tidReservert(tid,nr)
!nyAvtale(tid,nr)
?nyAvtale(tid,nr)
!tidIkkeOK(tid,nr)
?tidIkkeOK(tid,nr)
!finnNyLedigTid(tid,nr)
?finnNyLedigTid(tid,nr)
!tidReservert(tid,nr)
?tidReservert(tid,nr)

!nyAvtale(tid,nr)
?nyAvtale(tid,nr)
!tidOK(tid,nr)
?tidOK(tid,nr)
!bekreftAvtale(tid,nr)
?bekreftAvtale(tid,nr)>

Vi kunne selvfølgelig vist også de to siste tracene med nye antall iterasjoner av loopen, men viser i stedet to tracer fra diagrammene SykTannlege og TS_SykTannlege:

t4=
<!syk(tannlegeNr)
?syk(tannlegeNr)
!sykTannlege()
?sykTannlege()
!tannlegeSykUtsett?(tid,nr)
?tannlegeSykUtsett?(tid,nr)
!start(nr)
?start(nr)
!ikkeUtsett(tid,nr)
?ikkeUtsett(tid,nr)
!ikkeUtsett(tid,nr)
?ikkeUtsett(tid,nr)
!reset()
?reset()
!overtaTime(tid,nr)
?overtaTime(tid,nr)
!overtaTime(tid,nr)
?overtaTime(tid,nr)>

t5=
<!syk(tannlegeNr)
?syk(tannlegeNr)
!sykTannlege()
?sykTannlege()
!tannlegeSykUtsett?(tid,nr)
?tannlegeSykUtsett?(tid,nr)
!start(nr)
?start(nr)
!ikkeUtsett(tid,nr)
?ikkeUtsett(tid,nr)
!ikkeUtsett(tid,nr)
?ikkeUtsett(tid,nr)
!reset()
!overtaTime(tid,nr)
?reset()

?overtaTime(tid,nr)
!overtaTime(tid,nr)
?overtaTime(tid,nr)>

2 b.
Vi merker oss at det i sekvensdiagrammene ikke er definert noen negative tracer. Dermed slipper vi å argumentere for at bestemte tracer ikke kan produseres. Vår oppgave er å vise at dersom alle objekter av en annen klasse enn Pasient oppfører seg slik som beskrevet i sekvensdiagrammene, så vil det totale systemet oppføre seg slik som beskrevet i sekvensdiagrammene. Det vil si at vi må vise at Pasient ”gjør sin del av jobben”.

Vi tar først for oss diagrammet Innkalling (inkludert dekomposisjoner og refererte diagrammer).
Som utgangspunkt antar vi at tilstandsmaskinen av type Pasient (heretter bare kalt Pasient) starter i tilstand Venter når sekvensdiagrammet starter, og at attributtene ”avtale” og avtaleIntervall har gyldige verdier.

Vi antar at pasientens tannlege er frisk og at det derfor ikke kommer noen sykTannlege()-melding. Da vil Pasient stå i tilstand Venter helt til guard-betingelsen now>avtale+avtaleIntervall går fra usann til sann. Da sender Pasient ut meldingen trengerAvtale(nr) og går til tilstand VenterPåAvtale.

Tilstand for Pasient: VenterPåAvtale
Foreløpig produsert trace:
<!trengerAvtale(nr)>

Vi antar nå at omgivelsene til Pasient oppfører seg i henhold til sekvensdiagrammene, d.v.s. at Tannlege mottar ?trengerAvtale(nr) og sender tidReservert(tid, nr) til Pasient. Når Pasient mottar denne meldingen sender den ut meldingen nyAvtale(tid.nr) til PasientMobil og går til tilstand VenterPåBekreftelse.

Tilstand for Pasient: VenterPåBekreftelse
Foreløpig produsert trace:
<!trengerAvtale(nr)
?trengerAvtale(nr)
!tidReservert(tid,nr)
?tidReservert(tid,nr)
!nyAvtale(tid,nr)>

Antagelsen om at omgivelsene oppfører seg i henhold til sekvensdiagrammene forteller oss nå at det neste som skjer er at PasientMobil mottar ?nyAvtale(tid,nr). Deretter kan èn av to ting skje: a) PasientMobil sender tidOK(tid,nr) til Pasient eller b) PasientMobil sender tidIkkeOK(tid,nr) til Pasient.

Vi forfølger først alternativ a): Når Pasient står i tilstand VenterPåBekreftelse og mottar ?tidOK(tid,nr), sender den ut meldingen !bekreftAvtale(tid, nr) til Tannlege og går

deretter til tilstand Venter. Mottak av meldingen ?bekreftAvtale(tid, nr) er det siste som skjer i sekvensdiagrammet.

Tilstand for Pasient: Venter
Produsert trace:
<!trengerAvtale(nr)
?trengerAvtale(nr)
!tidReservert(tid,nr)
?tidReservert(tid,nr)
!nyAvtale(tid,nr)
?nyAvtale(tid,nr)
!tidOK(tid,nr)
?tidOK(tid,nr)
!bekreftAvtale(tid,nr)
?bekreftAvtale(tid,nr)>

Vi har nå vist at t1 kan produseres.

Så forfølger vi alternativ b): Når Pasient står i tilstand VenterPåBekreftelse og mottar ?tidIkkeOK(tid,nr), sender den ut meldingen !finnNyLedigTid(tid, nr) til Tannlege og går deretter til tilstand VenterPåAvtale.

Tilstand for Pasient: VenterPåAvtale
Foreløpig produsert trace:
<!trengerAvtale(nr)
?trengerAvtale(nr)
!tidReservert(tid,nr)
?tidReservert(tid,nr)
!nyAvtale(tid,nr)
?nyAvtale(tid,nr)
!tidIkkeOK(tid,nr)
?tidIkkeOK(tid,nr)
!finnNyLedigTid(tid, nr)

I følge sekvensdiagrammet vi da Tannlege motta denne meldingen og sende ut meldingen tidReservert(tid, nr) til Pasient. Pasient vil da sende ut meldingen !nyAvtale(tid,nr) til Pasientmobil og gå til tilstand VenterPåBekreftelse.

Tilstand for Pasient: VenterPåBekreftelse
Foreløpig produsert trace:
<!trengerAvtale(nr)
?trengerAvtale(nr)
!tidReservert(tid,nr)
?tidReservert(tid,nr)
!nyAvtale(tid,nr)
?nyAvtale(tid,nr)

!tidIkkeOK(tid,nr)
?tidIkkeOK(tid,nr)
!finnNyLedigTid(tid, nr)
?finnNyLedigTid(tid, nr)
!tidReservert(tid,nr)
?tidReservert(tid,nr)
!nyAvtale(tid,nr)

Nå ser vi at vi er tilbake til situasjonen hvor vi hadde de to mulighetene a) og b) som beskrevet over. Pasient er i nøyaktig samme tilstand som i det foregående tilfellet, og vi er på samme sted i sekvensdiagrammet (ved starten av loopen). Vi ser derfor at alle tracer på formen

<!trengerAvtale(nr)
?trengerAvtale(nr)
!tidReservert(tid,nr)
?tidReservert(tid,nr)
!nyAvtale(tid,nr)
?nyAvtale(tid,nr)
{!tidIkkeOK(tid,nr)
?tidIkkeOK(tid,nr)
!finnNyLedigTid(tid,nr)
?finnNyLedigTid(tid,nr)
!tidReservert(tid,nr)
?tidReservert(tid,nr)
!nyAvtale(tid,nr)
?nyAvtale(tid,nr)}*
!tidOK(tid,nr)
?tidOK(tid,nr)
!bekreftAvtale(tid,nr)
?bekreftAvtale(tid,nr)>

kan produseres, hvor {...}* angir at innholdet i parantesen kan gjentas 0-n ganger.

For å besvare oppgaven fullstendig måtte vi også gå gjennom sekvensdiagrammene for syk tannlege, men det dropper vi her.

2 c.

Gjennom å løse oppgave b har vi vist at systemet er en gyldig raffinering av spesifikasjonene fra oppgave 1 c. Siden vi ikke har brukt xalt, har vi kun ett obligasjonspar. Vi lar da semantikken til spesifikasjonen fra oppgave 1c være gitt ved {(p1, n1)} og spesifikasjonen av tilstandsmaskinene være {(p2, n2)}, dvs at alle tracer som kan produseres av tilstandsmaskinene er i mengden p2, mens alle andre tracer er i n2.

For å vise at vi har en raffinering må vi vise at $n1 \subseteq n2$ og $p1 \subseteq p2 \cup n2$.
Siden $n1 = \emptyset$, er $n1 \subseteq n2$ oppfyllt. Og siden $p2 \cup n2$ faktisk utgjør hele universet av tracer, er også $p1 \subseteq p2 \cup n2$ oppfyllt.

Dersom vi har vist at *alle* positive tracer fra sekvensdiagrammene kan produseres av tilstandsmaskinene (hvilket vi strengt tatt ikke har fullført), kunne vi konkludert med at vi har vi en supplementering, fordi vi da har oppfyllt både $n1 \subset n2$ og $p1 \subseteq p2$.

For å ha en narrowing måtte følgende være oppfyllt:

1. $n1 \subset n2$
2. $p2 \subset p1$
3. $n2 = n1 \cup (p1 \setminus p2)$

For å oppfylle 2. måtte vi i vår simulering vise at det er minst ett positivt trace fra sekvensdiagrammene som *ikke* kan produseres av tilstandsmaskinene (hvilket vi ikke kan her så lenge vi har antatt at alle andre tilstandsmaskiner enn :Pasient oppfører seg som beskrevet av sekvensdiagrammene).

Retteinstruks til oppgave 3

.
Pasientforeningen i samarbeide med helsedirektoratet ønsker en sikkerhetsvurdering av systemet. Målet er å sikre at pasientenes interesser blir ivaretatt.

a) (2%) Hvilke av følgende aktiva er relevante for en slik analyse (begrunn svaret):
    a. Tannlegesenterets kundemasse
    b. Pasientens helse
    c. Pasientens omdømme
    d. Informasjon i tannlegesenterets arkiv
    e. Tannlegesenterets økonomi
    f. Pasientens privatliv

Definisjon: et aktiva er noe som har verdi for en interessent vi gjennomfører analysen på vegne av.

Eksempel: for en pasient vil pasientjournalen hans/hennes være verdifull og dermed anses som et aktivum.

Krav: her er det pasientforeningen og helsedirektoratet som på vegne av pasienten bestiller analysen og dermed regnes pasienten som interessenten. Aktiva defineres ut ifra hva interessenten anser som verdifullt, de riktige alternativer er:
b) Pasientens helse,
c) Pasientens omdømme (omdømmet kan lide hvis sensitiv informasjon om pasienten lekker ut),
d) Info i tannlegesenterets arkiv (verdifull for pasienten pga sitt sensitive innhold) ,

f) Pasientens privatliv (hvis info i tannlegesenteret kan skade dette privatlivet)

De to utelatte er aktiva for tannlegesenteret, fokus i denne analyse er derimot pasienten.

Poengtildeling: maks 2 poeng. 2 poeng for fire riktige, 1 poeng for 3 riktige. Det skal trekke ned å "helgardere" ved å velge alle.

SensorTic:

1. Klarer kandidaten å skille ut aktiva relevante for pasienten?

   ☐Ja ☐Delvis ☐Nei
2. Hvis delvis eller nei på forrige, hvilken av de andre potensielle interessentene blander kandidaten inn?

   ☐Tannlegesenteret ☐Sosial- og helsedirektoratet ☐Annet

b) (2%) Definer fem kvalitative frekvensverdier du vil bruke i denne analysen. Beskriv hvordan disse skal tolkes (i form av kvantitative sannsynligheter)

Definisjon: En frekvensverdi sier hvor hyppig risken antas å oppstå.
Eksempel: Vår forslag til frekvensverdier i form av sannsynligheter er følgende:

- Usannsynlig (U): [0.0, 0.001]
- Lite sannsynlig (Ls): < 0.001, 0.005]
- Ganske sannsynlig (Gs): < 0.005, 0.1]
- Sannsynlig (S): < 0.1, 0.6]
- Veldig sannsynlig (Vs): < 0.6, 1]

Krav: kandidaten skal ha en noenlunde tilsvarende skala med fem frekvensverdier, men her brukes normal sensorskjønn for å avgjøre om skalaen er fornuftig.

Poengtildeling: maks 2 poeng. 2 poeng gis for fem frekvenskvensverdier på en fornuftig skala som starter med frekvensverdi tilnærmet null. Trekk hvis den kvalitative betegnelsen ikke henger logisk sammen med den kvantitative, dvs. usannsynlig bør ikke ha en unaturlig høy P.

SensorTic:

3. I hvilken grad har du inntrykk av at kandidaten har forstått hva en *kvalitativ* frekvensverdi er?

   Godt ☐ ☐ ☐ ☐ ☐ Dårlig
4. I hvilken grad har du inntrykk av at kandidaten har forstått hva en *kvantitativ* frekvensverdi er?

   Godt ☐ ☐ ☐ ☐ ☐ Dårlig
5. Hvordan deler kandidaten opp P i intervaller?

☐ fem like store utfallsrom

☐ korte i ytterkantene, større mot midten

☐ som vi har gjort i vårt forslag, korte intervaller i bunnen, større oppover skalaen

☐ annet

c) (2%) Definer tre konsekvensverdier du vil bruke i denne analysen. Beskriv hvordan disse skal tolkes i praksis

Definisjon: En konsekvensverdi angir hvor skadelig en risk er antatt å være.

Eksempel: Vårt forslag er til skala for pasienten i forhold til tannlegesystemet er:

- Liten konsekvens: tap av verdi for pasient < 1000kr,
- Medium konsekvens: tap av verdi for pasient >= 1000 kr, < 10 000kr
- Alvorlig konsekvens: tap av verdi for pasient >= 10 000kr

Krav: kandidaten må oppgi minst 3 og at steget mellom hver av dem må være naturlig, dvs. man hopper ikke fra liten konsekvens til alvorlig konsekvens uten å ha noe i mellom. Dette er som sagt et forslag til konsekvensverdier, det er både lov til å definere andre og flere. I dette tilfellet skal skalaen gjenspeile at det er en pasient som taper penger her, ikke en stor og rik organisasjon. Man skal regne med at et tap på over 10 000kr for en pasient oppfattes som en alvorlig konsekvens, dvs skalaen med tapsbeløp skal være relativ lav.

Poengtildeling: maks 2 poeng. Det gis 2 poeng for 3 konsekvensverdier på en jevnt stigende og fornuftig skala som starter med lav konsekvensverdi. Trekk hvis skalaen ikke gjenspeiler pasienten som interessent, eller hvis det ikke oppgis minst 3 konsekvensverdier.

SensorTic:

6. Har kandidaten oversatt konsekvensverdiene til pengebeløp?

   ☐Ja ☐Delvis ☐Nei

7. I hvilken grad har kandidaten lagt den praktiske skalaen slik at den passer en pasient?

   Passer godt ☐ ☐ ☐ ☐ ☐ Passer dårlig

d) (2%) Definer kvalitative risikoverdier for denne analysen og relater de til frekvensene og konsekvensene du har definert over

Definisjon: En risikoverdi er en funksjon av frekvens og konsekvens. Den angir "alvorlighetsgraden" på risken.

Eksempel: tre av de mest vanlige kvalitative verdier er:

- liten risk
- medium risk
- alvorlig risk

Når man skal relatere disse til frekvens og konsekvensverdier brukes for eksempel en risikoverdi-matrise som den under.

Risikoverdi-matrise	**Frekvens**				
	Usannsynlig	**Lite**	**Ganske**	**Sannsynlig**	**Veldig**

			sannsynlig	sannsynlig		sannsynlig
Konsekvens	**Liten**	Lav risko	Lav risko	Medium risiko	Medium risiko	Høy risiko
	Medium	Lav risko	Medium risiko	Medium risiko	Høy risiko	Høy risiko
	Alvorlig	Medium risiko	Medium risiko	Høy risiko	Høy risiko	Høy risiko

Krav: her er det viktig at de samme frekvens- og konsekvensverdier som kandidaten har oppgitt i opg 2 og 3 går igjen i matrisen, og at inndelingen mellom de ulike risikoverdi-områdene (lav-grønn, medium-gul, høy-rød) er fornuftig (dvs at alvorlig konsekvens <--> ganske sannsynlig bør få risikoverdi høy, ikke medium). Det kreves egentlig ikke at det lages en slik matrise hvis kandidaten får forklart tilsvarende på annen måte, men dette er nok den enkleste og beste løsningen. Det kreves heller ikke at matrisen farges..

Poengtildeling: maks 2 poeng. Trekk hvis ikke frekvens- og konsekvensverdier tilsvarer svarene på opg 2 og 3, og hvis inndelingen av matrisen er ulogisk.

SensorTics:

8. I hvilken grad virker det som om kandidaten har forstått at risikoverdi utledes fra konsekvens og frekvens?

   Godt ☐ ☐ ☐ ☐ ☐ Dårlig

9. I hvilken grad deler kandidaten inn funksjonen i fornuftige seksjoner (lav, medium, høy risiko)?

   Fornuftig ☐ ☐ ☐ ☐ ☐ Lite fornuftig

e) (3%) Spesifiser minst tre risikoakseptanskriterier (risikoevalueringskriterier) for denne analysen

Definisjon: Et risiko-akseptanskriterium karakteriserer hva man kan tolerer med hensyn til risk.

Eksempel: de mest vanlige her er:

- aksepter risk
- monitorere/overvåke risk
- behandle risk.

En måte å relatere disse verdiene til konsekvens og frekvensverdiene er å lage en risikoakseptans-matrise av typen vist under.

Risikoakseptans-matrise		**Frekvens**				
		Usannsynlig	**Lite sannsynlig**	**Ganske sannsynlig**	**Sannsynlig**	**Veldig sannsynlig**
Konsekvens	**Liten**	Aksepter risiko	Aksepter risiko	Overvåk risiko	Overvåk risiko	Behandle risiko

	Medium	Aksepter risiko	Overvåk risiko	Overvåk risiko	Behandle risiko	Behandle risiko
	Alvorlig	Overvåk risiko	Overvåk risiko	Behandle risiko	Behandle risiko	Behandle risiko

Kriteriene kan også formuleres direkte uten bruk av matrise. Det er ikke uvanlig å sette opp ulike kriterier for ulike aktiva.

Krav: Kriteriene skal formuleres med hensyn til de samme risikoverdiene som ble definert av kandidaten tidligere. Kriteriene skal spesifisere hva den man gjennomfører analysen for kan tolerere av tap. Hva som krever behandling.

Poengtildeling: maks 3 poeng. Trekk hvis ikke risikoakseptanskriteriene tilsvarer risikoverdiene (evt aktiva) definert tidligere.

SensorTics:
10. I hvilken grad har kandidaten definert kriteriene fornuftig?

Fornuftig ☐ ☐ ☐ ☐ ☐ Lite fornuftig

f) (3%) Identifiser fem uønska hendelser med hensyn til de aktiva som du har angitt som relevante under Opg. 3a

Definisjon: En uønsket hendelse er noe som kan skade et aktivum.

Eksempel:

Uønsket hendelse
Klientens kredittkort misbrukes
Datautstyr hvor Appointment System er deployet blir stjålet
Uvedkommende finner opplysninger om klienter på stjålne datamaskiner

Krav: Her må den uønskede hendelsen være fornuftig og relatert til et av de aktiva kandidaten valgte i opg 3a.

Poengtildeling: maks tre poeng. 3 poeng for fem uønskede hendelser, 2 poeng for tre eller fire, 1 poeng for en eller to.

SensorTic:
11. Spesifiserte kandidaten hvilket aktivum den uønskede hendelsen relaterte seg til?

☐Ja ☐ Delvis ☐ Nei

g) (3%) Definer relevante trusler, trusselscenarioer og sårbarheter for de uønskede hendelsene du identifiserte i opg 3f.

Definisjon: En trussel er noe eller noen som utnytter en sårbarhet for å gi opphav til/sette igang en uønsket hendelse. En sårbarhet er en svakhet eller mangel. Et trusselscenario er en beskrivelse av hvordan trusselen utnytter sårbarheten.

Eksempel:

Trussel	Trusselscenario	Sårbarhet	Uønsket hendelse
Eavesdropper	Kredittkortnummer fanges opp	Mangler kryptering	Klientens kredittkort misbrukes
Kjeltring	Innbrudd	Ulåst rom	Datautstyr hvor Appointment System er deployet blir stjålet
Kjeltring	Innbrudd	Ukryptert data	Uvedkommende finner opplysninger om klienter på stjålne datamaskiner

Krav: her kreves det at alle de uønskede hendelsene kandidaten identifiserte i oppgave 3f er nevnt i en trussel-sårbarhetskombinasjon.

Poengtildeling: maks 3 poeng.

SensorTics:

12. I hvilken grad har du inntrykk av at kandidaten har forstått begrepet ”trussel”?

    Godt ☐ ☐ ☐ ☐ ☐ Dårlig

13. I hvilken grad har du inntrykk av at kandidaten forstår sammenhengen mellom trussel og sårbarhet?

    Godt ☐ ☐ ☐ ☐ ☐ Dårlig

h) (3%) Forklar på hvilken måte én og samme uønska hendelse gi opphav til flere risikoer

Definisjon: En uønsket hendelse er en del av en risk og assosieres med de/det aktivumet den kan skade. En uønsket hendelse kan igangsette flere risker hvis den er assosiert med flere aktiva (én pr aktiva).

Eksempel:
- Tannlegesenteret kan fks. oppbevare selve pasientjournalen ett sted og personlig informasjon om pasienten et annet sted, hvis den uønskede hendelsen skjer at en inntrenger kommer seg inn i datasystemet kan han/hun få tak i begge disse aktivaene, og dermed gir denne uønskede hendelsen opphav til to ulike risikoer.

En uønsket hendelse gir opphav til mer enn risk hvis den reduserer verdien av mer enn et aktivum.

Krav: besvarelsen må ha med at en risk består av en uønsket hendelse, dens frekvens og konsekvens, Konsekvensen er alltid med hensyn til kun et aktivum. Det betyr at hvis den samme uønskede hendelsen har konsekvens for flere aktiva så gir den opphave til flere risker.

Poengtildeling: Max 3 poeng, normalt sensorskjønn må benyttes for gradering. Det gis ikke poeng for tilfellet der en uønsket hendelse initierer en ny uønsket hendelse, her er det én og samme uønsket hendelse som gjelder.

SensorTic:

14. På hvilken måte begrunner kandidaten dette svaret?

    ☐ én uønsket hendelse assosiert med flere aktivum gir flere risikoer

    ☐ en uønsket hendelse kan igangsette nye uønskede hendelser og dermed gi opphav til flere risikoer

    ☐ annet

15. I hvilken grad har kandidaten forstått at en uønsket hendelse er en del av en risiko?

    Godt ☐ ☐ ☐ ☐ ☐ Dårlig

i) (3%) Definer minst **åtte** risikoer for de **fem** uønska hendelsene du definerte i opg 3f slik at halvparten krever behandling

Definisjon: En risiko består av en uønsket hendelse, en frekvensverdi og en konsekvensverdi. Frekvens og konsekvens vil til sammen gi risikoverdien.

Eksempel: Siden det bes om flere risikoer enn man har enkeltvise uønskede hendelser må flere uønskede hendelser være assosiert med samme aktivum. Hvis vi tar eksempelet fra forrige opg inneholder det en uønsket hendelse (inntrenger på datasystemet) som berører to aktivumer (pasientjournal og pasientopplysninger) som dermed kan gi opphav til to risikoer:
1) inntrenger på datasystemet får tilgang til pasientjournal, frekvens: lite sannynlig, konsekvens: medium, risikoverdi=medium risko (ihh til risikoverdimatrise), reaksjon: overvåk risko (ihh til risikoakseptans-matrise).
2) inntrenger får tilgang til pasientinformasjon, frekvens: lite sannsynlig, konsekvens: alvorlig, risikoverdi= alvorlig risiko (ihh til risikoverdimatrise), reaksjon: må behandles (ihh til risikoakseptans-matrise).

Krav: hver risiko må ha definert frekvens, konsekvens og risikoverdi for å godtas som svar. Det er viktig at de riskene som krever behandling faktisk har risikoverdi som gjenspeiler risiko-akseptanskriteriene til kandidaten.

Poengtildeling: 3 poeng for åtte eller flere risikoer, 2 poeng for 6-7, 1 poeng for 4-5, 0 poeng for færre risikoer enn 4.

SensorTic:

16. Har kandidaten forstått at en risiko består av en uønsket hendelse, konsekvens og frekvens?

    ☐ Ja

    ☐Delvis, oppgir ikke risikoverdi

    ☐Delvis, oppgir ikke frekvens

☐Delvis, oppgir ikke konsekvens

☐Delvis, oppgir ikke uønsket hendelse

☐Nei

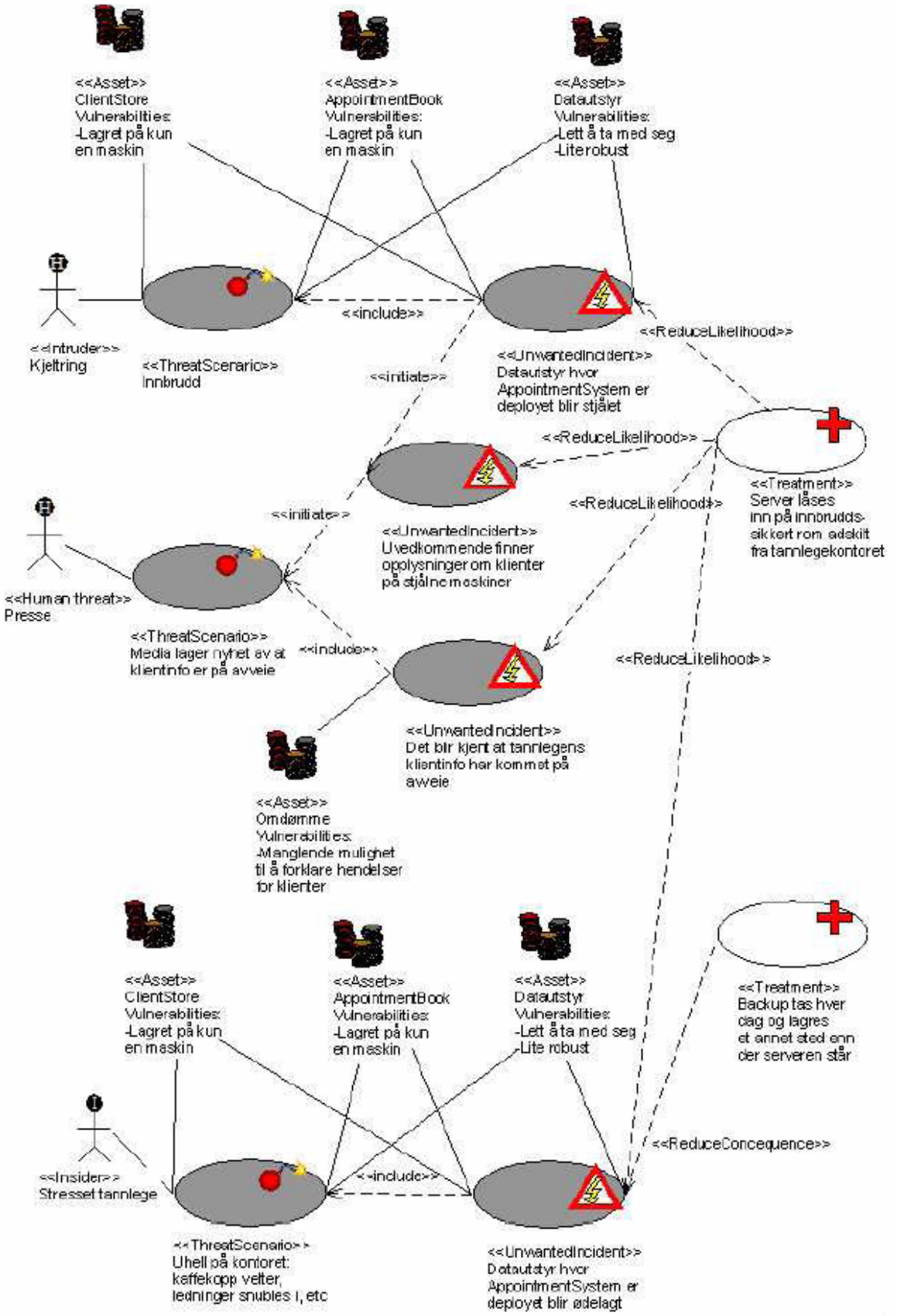
17. I hvilken grad har kandidaten forstått at risikoverdi utledes fra konsekvens og frekvensverdiene han/hun har definert tidligere?

Godt ☐ ☐ ☐ ☐ ☐ Dårlig

j) (7%) Dokumenter behandlingen av risikoene ved hjelp av diagrammer uttrykt i CORAS profilen. Det er nok at diagrammene beskriver hvordan de relevante truslene, trusselscenarier, aktiva, uønska hendelser og behandlinger relaterer seg til hverandre

Eksempel:[2]

[2] Diagrammet er ok, men jeg hadde fjernet assosiasjonene mellom aktiva og uønska hendelser for de 6 aktiva som også har en assosiasjon med et trusselscenario. De seks assosiasjonene som fjernes følger nemlig implisitt fra include-relasjonen.


<<Asset>>
ClientStore
Vulnerabilities:
-Lagret på kun
en maskin
<<Asset>>
AppointmentBook
Vulnerabilities:
-Lagret på kun
en maskin
<<Asset>>
Datautstyr
Vulnerabilities:
-Lett å ta med seg
-Lite robust
<<include>>
<<ReduceLikelihood>>
<<Intruder>>
Kjeltring
<<ThreatScenario>>
Innbrudd
<<initiate>>
<<UnwantedIncident>>
Datautstyr hvor
AppointmentSystem er
deployet blir stjålet
<<ReduceLikelihood>>
<<Treatment>>
Server låses
inn på innbrudds-
sikkert rom adskilt
fra tannlegekontoret
<<initiate>>
<<UnwantedIncident>>
Uvedkommende finner
opplysninger om klienter
på stjålne maskiner
<<ReduceLikelihood>>
<<Human threat>>
Presse
<<ThreatScenario>>
Media lager nyhet av at
klientinfo er på avveie
<<include>>
<<ReduceLikelihood>>
<<UnwantedIncident>>
Det blir kjent at tannlegens
klientinfo har kommet på
avveie
<<Asset>>
Omdømme
Vulnerabilities:
-Manglende mulighet
til å forklare hendelser
for klienter
<<Asset>>
ClientStore
Vulnerabilities:
-Lagret på kun
en maskin
<<Asset>>
AppointmentBook
Vulnerabilities:
-Lagret på kun
en maskin
<<Asset>>
Datautstyr
Vulnerabilities:
-Lett å ta med seg
-Lite robust
<<Treatment>>
Backup tas hver
dag og lagres
et annet sted enn
der serveren står
<<ReduceConcequence>>
<<Insider>>
Stresset tannlege
<<include>>
<<ThreatScenario>>
Uhell på kontoret:
kaffekopp velter,
ledninger snubles i, etc
<<UnwantedIncident>>
Datautstyr hvor
AppointmentSystem er
deployet blir ødelagt

Krav: her kreves det at alle nevnte elementer gjengis ihh til det kandidaten har definert tidligere i oppgaven, dvs her skal det ikke komme nye elementer bortsett fra behadlingsalternativene.

Om notasjon:

- Kun stiplede assosiasjoner har ”pil-ending”.
- Pilen fra en uønsket hendelse skal peke mot inkluderte trusselscenarioer, ikke omvendt. Den kan også peke på andre uønskede hendelser hvis den uønskede hendelsen initierer disse.
- Pilen fra behandlingen skal peke mot en uønsket hendelse eller en trussel eller en sårbarhet ved et aktivum (hvis dette er oppgitt) avhengig av hvor behandlingen settes inn. Det er lovlig å angi behandlingseffekten på selve pilen.
- En heltrukket assosiasjon uten pil på kan enten gå mellom en uønsket hendelse og et aktivum eller mellom et aktivum og et trusselscenario.
- Mellom trussel og trusselscenario skal det være relasjon uten pil på.

Krav til notasjon: det skal vektlegges et fullstendig diagram fremfor korrekt bruk av stiplet/heltrukket/med pil og uten pil-assosiasjoner. Det er heller ikke krav om korrekt stereotyping av elementene så lenge det er mulig å skille en uønsket hendelse fra fks et aktivum.

Poengtildeling: maks 7 poeng. Her må sensor bruke skjønn i forhold til kravene som er satt opp. Hvis man i tillegg til å ha et godt diagram også:

- beskriver sårbarheter ved aktivumene
- tar med behandlingseffekt på pilen fra behandlingsalternativet (slik som i eksemplediagrammet).

bør dette krediteres.

SensorTic:

18. Har kandidaten unnlatt å modeller noe av følgende begreper (sett kryss)?

	Ja	Delvis
trusler:		
trusselscenarier:		
aktiva:		
uønska hendelser		
behandlinger:		

19. Har kandidaten brukt heltrukne assosiasjoner?

☐ Ja ☐ Nei

20. Har kandidaten brukt stiplete pil-assosiasjoner?

☐ Ja, mellom behandling og uønsket hendelse

☐ Ja, mellom uønsket hendelse og trusselscenario

☐ Ja, andre steder

☐ Nei

21. Har kandidaten beskrevet behandlingseffekten i diagrammet (på linjen fra behandling mot et annet element)?

    ☐ Ja ☐ Nei

22. I hvilke grad virker det som om kandidaten har forstått at et trusselscenario er inkludert i en uønsket hendelse og modellert deretter? (den stiplete assosiasjonen er merket med <<include>> og peker **fra** uønsket hendelse **mot** trusselscenario)

    Godt ☐ ☐ ☐ ☐ ☐ Dårlig

k) (5%) Hvorfor det er viktig å kunne uttrykke eksplisitt ikke-determinisme når man skal bygge et tannlegesystem som ivaretar sikkerhet. Illustrer dette i form av et sekvensdiagram.

Fordi eksplisitt ikke determinisme er et middel til økt sikkerhet.

Anta for eksempel at man ønsker å gi hver pasient en aksesskode for ytterdør på tannlegesenteret. Denne aksesskoden, et tall på 4 siffer, sendes til pasienten når denne aksepterer timetilordning. Aksesskoden vil kun fungere den dagen pasienten har time.

En slik aksesskodegenerator kan man for eksempel spesifisere som en loop over en xalt med 10 operander (en for hvert tall mellom 0 og 9).