# UNIVERSITETET I OSLO

## Det matematisk-naturvitenskapelige fakultet

**Exam in - INF5150**
**Day of exam: 5. December 2006**
**Exam hours: 15.30 – 18.30**
**This examination paper consists of …page(s).**
**Appendices:**
**Permitted materials: All written material.**

*Make sure that your copy of this examination paper is complete before answering.*

**NB: This exam text is only given in English since the course has been given in English this year. The candidate may, however, choose to answer in Bokmål or Nynorsk if he or she wants.**

## Weather service

The business idea behind this service is that people send weather reports from wherever they are, and in return they immediately get weather forecasts for their spot based on all the collected weather reports. The collected weather reports also include data received from weather sensors that periodically send weather reports via SMS to the central database.

The weather forecast is given to the requester by SMS and the collected reports can possibly be viewed on GoogleEarth since the observations are optionally placed in a KML-file.

It is not important for this exam, but we imagine that the weather forecast is done by calculating the routes of the weather and projecting the weather by what is before the requester. For example if the weather seems to flow to Oslo from the west over Drammen we can project that the weather in Oslo will in a few hours be like the weather is now in Drammen. Thus the requester in Oslo takes advantage of the reporters in Drammen.

The exercises may be answered in any order as they should be reasonably independent, but they do refer to the Weather service and Figure 1 for context.

### *1 Modeling (35%)*

In Figure 1 there is a sequence diagram specifying a situation of the Weather Context. Please notice that the uppermost combined fragment has the operator **par**.

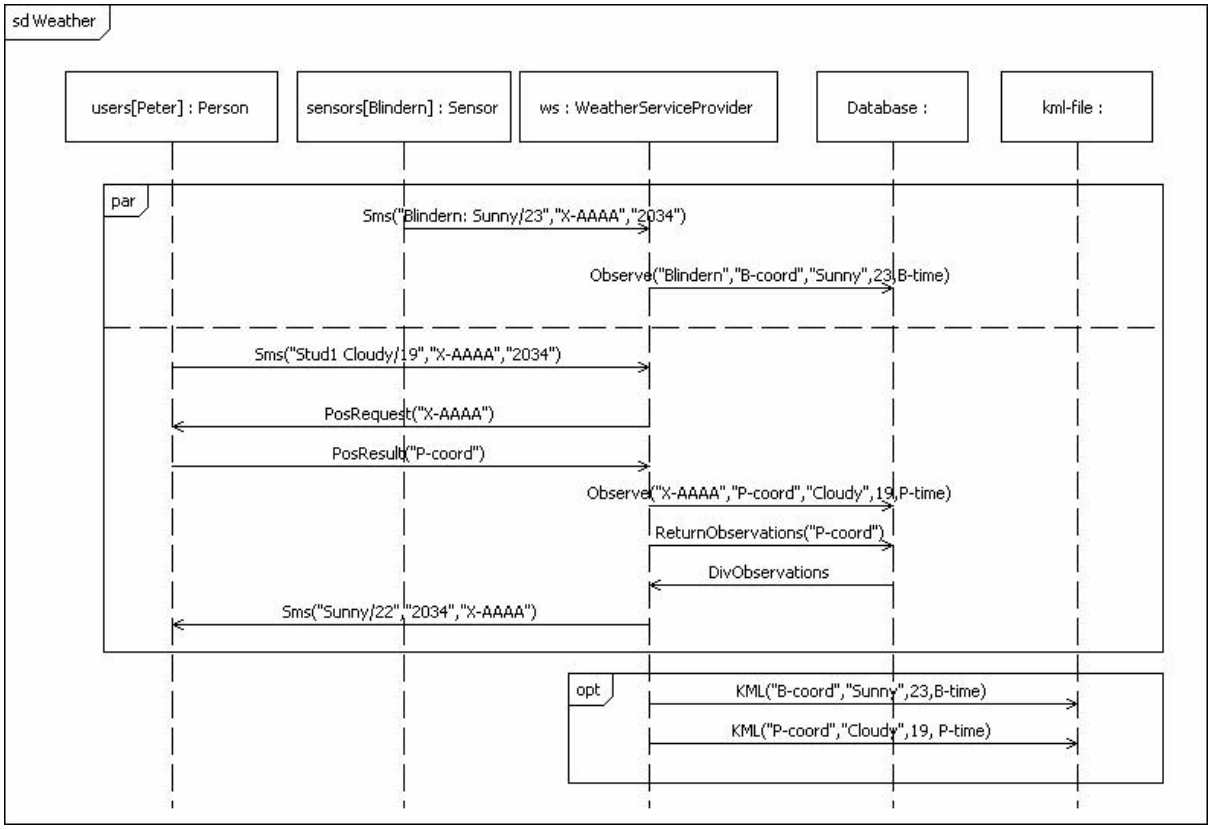



**Figure 1Weather reporting and forecasting scenario**

The corresponding composite structure of the context is given in Figure 2.

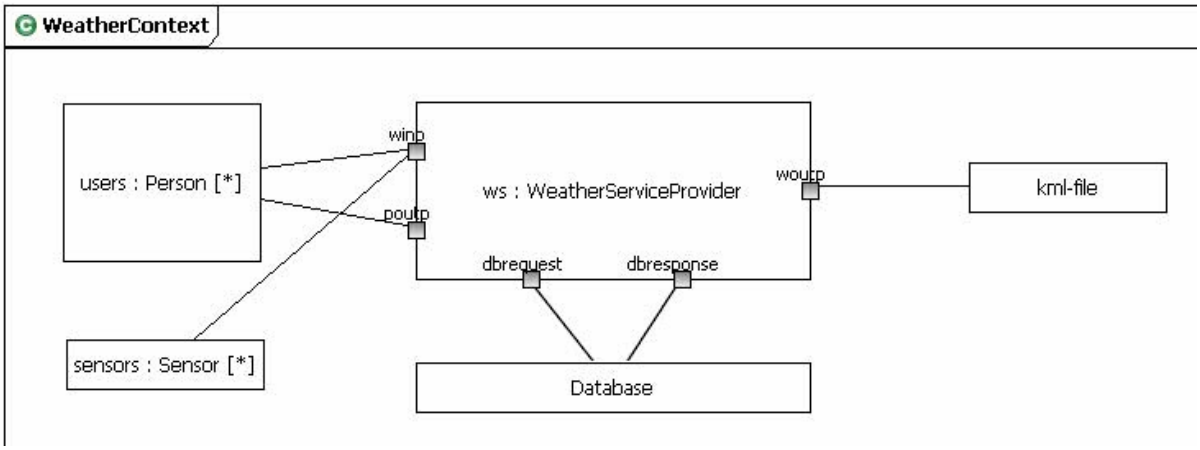
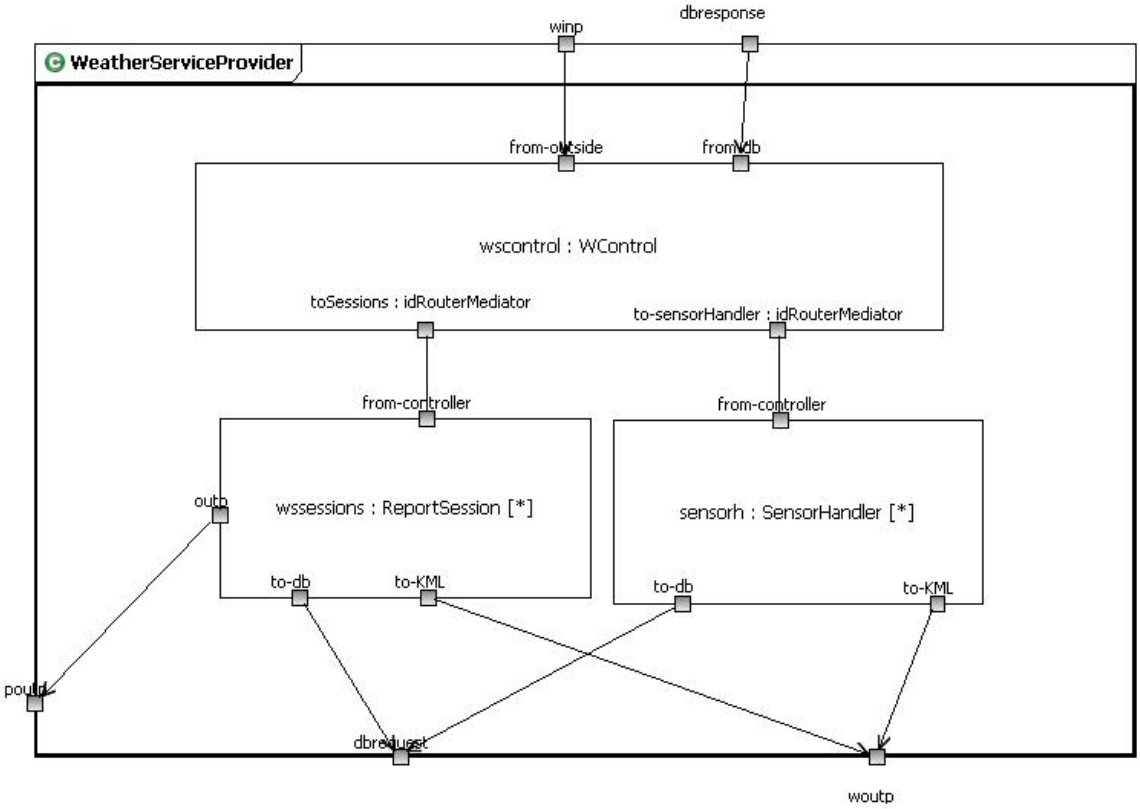



**Figure 2Weather context composite structure**

## 1 a) Composite structure

Define a composite structure for WeatherServiceProvider where each sensor is handled by a state machine and there is a session for each weather report sent on SMS from some mobile phone.

## 1 a) Solution: Composite structure




**Signal flow**
As this composite shows, the flow of signals is unidirectional in this supposed architecture. All signals entering the system is handled by the WControl, and all signals sent out of the system are done by either a ReportSession or the SensorHandler.

**WControl**
This part works mainly as a signal router ensuring that the signals from users, PATS and the database end up at the right place. WControl creates and organizes all the ReportSessions. They are identified through unique SessionIds, and the routing is done by a SimpleRouterMediator.

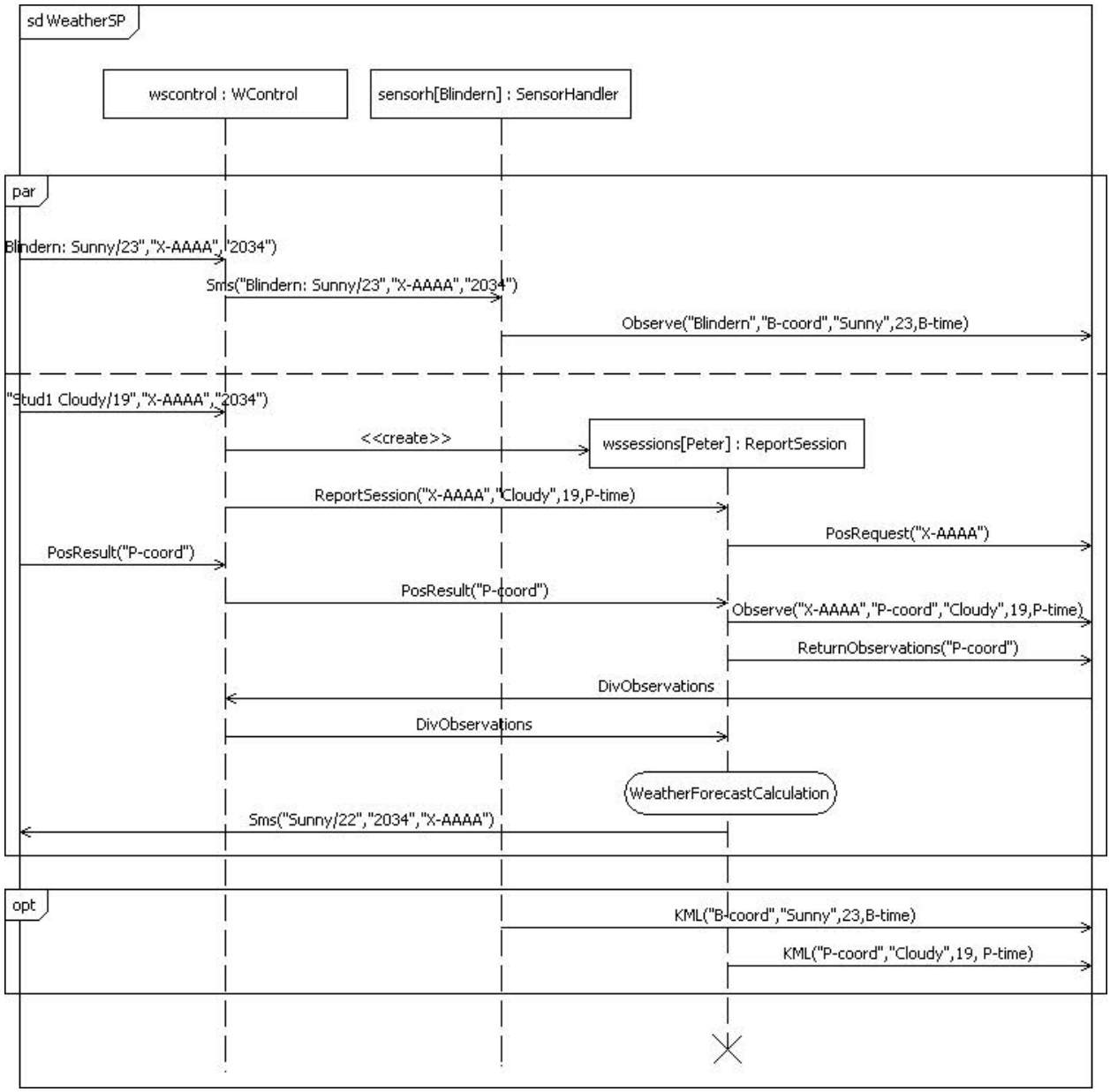
**ReportSession**
This part has multiplicity many, and a instance of this part/state machine will be create for every weather report submitted by a user.

**SensorHandler**
This part has multiplicity many, and there is an instance of this part for each of the sensors. The exam suggests that this part is implemented by the state machine given in Figure 3. To improve the architecture I have chosen to assume that the part is implemented by a more complex state machine by adding handling of KML-file updates in addition to the communication with the database.

## 1 b) Decomposition

Define a decomposition of lifeline WeatherServiceProvider for sequence diagram Weather.

## 1 b) Solution: Decomposition




**Comments**

It is assumed that sessionIDs a generated by WControl and used to identify the different sessions.

The KML-file update and the forecast calculation could have been done by WControl, but I have chosen to give the controller only routing functionality. This means that I have assumed that sensorHandler is implemented by a more complex state machine than the one given in Figure 3 in the exam.

## 1 c) State machine

In Figure 3 there is the state machine for the weather sensor corresponding to the sequence diagram in Figure 1. We include this state machine to show some of the vocabulary in the transitions, and how possible variables can be shown.

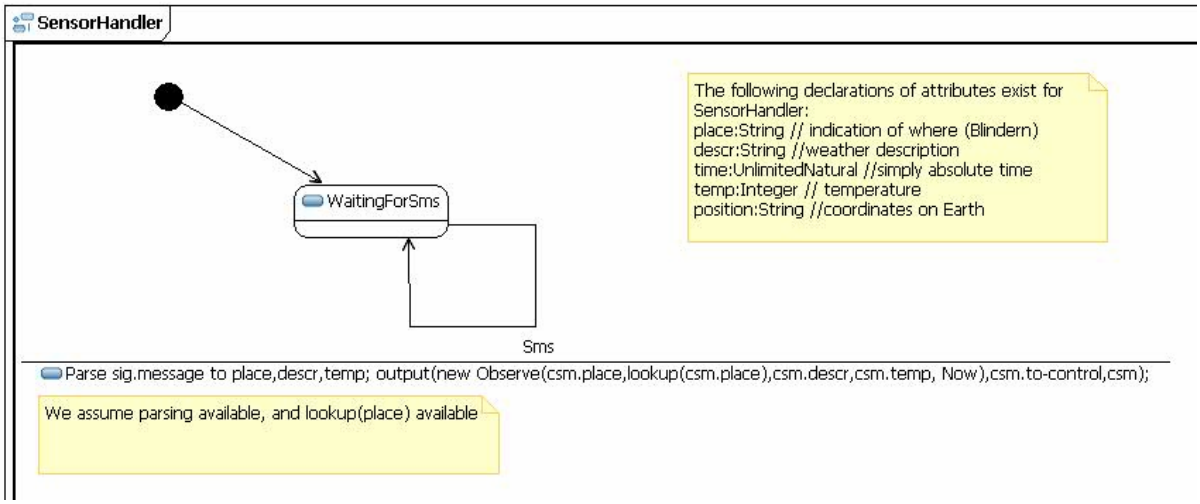
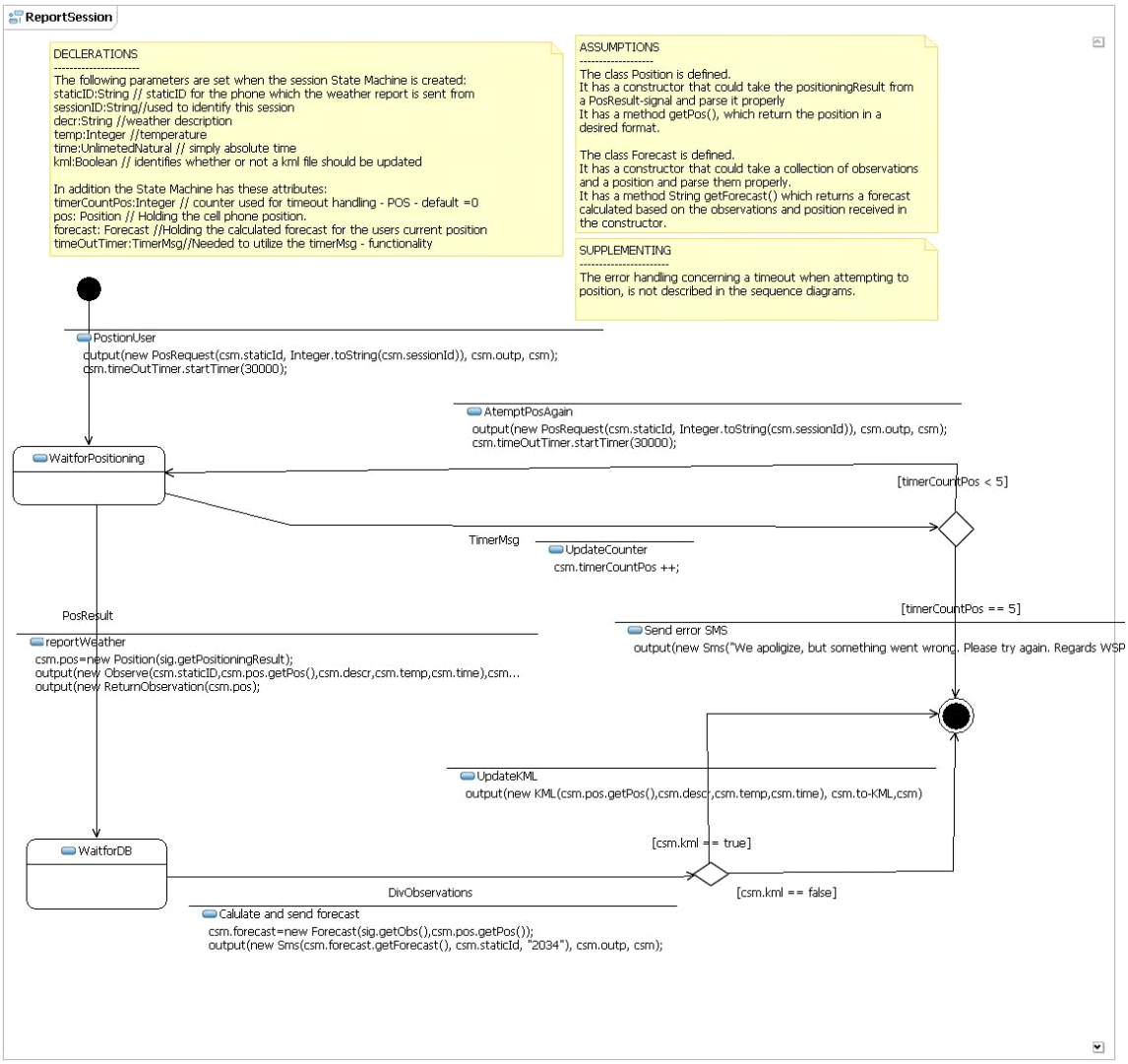



**Figure 3State Machine for SensorHandler**

Make a state machine for a weather report session.

## 1 c) Solution: State machine



## COMMENTS (SAME AS THOSE IN THE DIAGRAM)

### Declarations

The following parameters are set when the session State Machine is created:
staticID:String // staticID for the phone which the weather report is sent from
sessionID:String//used to identify this session
decr:String //weather description
temp:Integer //temperature
time:UnlimetedNatural // simply absolute time
kml:Boolean // identifies whether or not a kml file should be updated

In addition the State Machine has these attributes:
timerCountPos:Integer // counter used for timeout handling - POS - default =0
pos: Position // Holding the cell phone position.
forecast: Forecast //Holding the calculated forecast for the users current position
timeOutTimer:TimerMsg//Needed to utilize the timerMsg - functionality

### Assumptions

The **class Position** is defined.
It has a constructor that could take the positioningResult from a PosResult-signal and parse it properly
It has a method getPos(), which return the position in a desired format.

The **class Forecast** is defined.
It has a constructor that could take a collection of observations and a position and parse them properly.
It has a method String getForecast() which returns a forecast calculated based on the observations and position received in the constructor.

### Supplementing

The error handling concerning a timeout when attempting to position, is not described in the sequence diagrams.

## *2 STAIRS (35%)*

The exercises below refer to the sequence diagram of Figure 1, but do not depend on what you have answered on exercise 1 above.

### 2 a) Events

STAIRS Tutorial associates two events with each message, a send event and a reception event.

I. What is the first event(s) of Figure 1. Explain your answer.

*There are two possible first events: !Sms(“Blindern: Sunny/23”,”X-AAAA”,”2034”) on lifeline sensors[Blindern]:Sensor and !Sms(“Stud1: Cloudy/19”,”X-AAAA”,”2034”) on lifeline users[Peter]:Person. These two events are the first event in the first and the second operand of the par operator. Both events may occur first since the traces of the operands of a par operator may be interleaved in any order.*

II. What is the last event(s)? Again explain your answer.

*There are three possible last events. If the contents of the opt operator is included then the last event will be*
*?KML(“P-coord”,”Cloudy”,19,P-time) on lifeline kml-file:.*

*If the contents of the opt operator is not included then the last event will be either*
*?Observe(“Blindern”,”B-coord”,”Sunny”,23,B-time) on lifeline Database: (this is the last event of the first par operand) or*
*?Sms(“Sunny/22”,”2034”,”X-AAAA”) on lifeline users[Peter]:Person (this is the last event of the second par operand).*
*Again the reason why both these traces may be the last trace is that the traces of the operands of a par operator may be interleaved in any order.*

### 2 b) Traces

I: How many positive traces are captured by the first operand of the **par**-construct of Figure 1.

*One trace.*

II: How many positive traces are captured by the second operand of the **par**-construct of Figure 1.

*Two traces. After !Observe(...), the next event could be either ?Observe(...) or !returnObservations(...)*

III: How many traces are negative with respect to the diagram in Figure 1. Explain your answer.

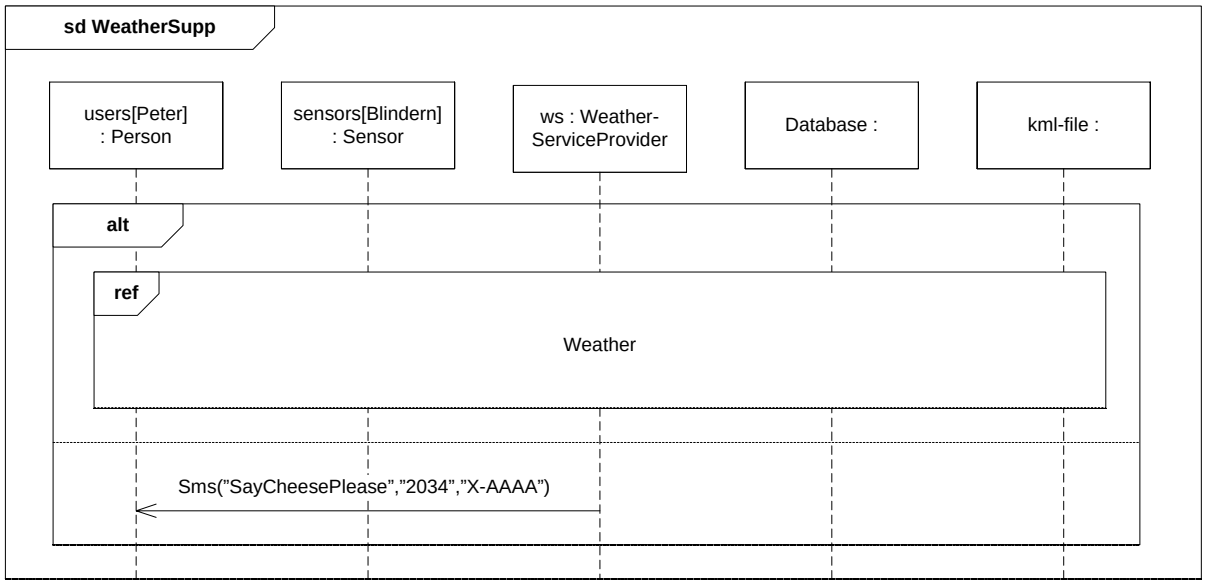
*No traces are negative w.r.t. the diagram in Figure 1, since neither neg, refuse, veto, assert, nor guards/constraints have been used.*

IV: How many traces are inconclusive with respect to the diagram in Figure 1. Explain your answer.

*Infinitely many traces are inconclusive, since the set of possible traces is infinite (independently of the diagram). Since the diagram specifies only a finite set of traces as positive or negative, the set of remaining (i.e. inconclusive) traces is necessarily infinite.*

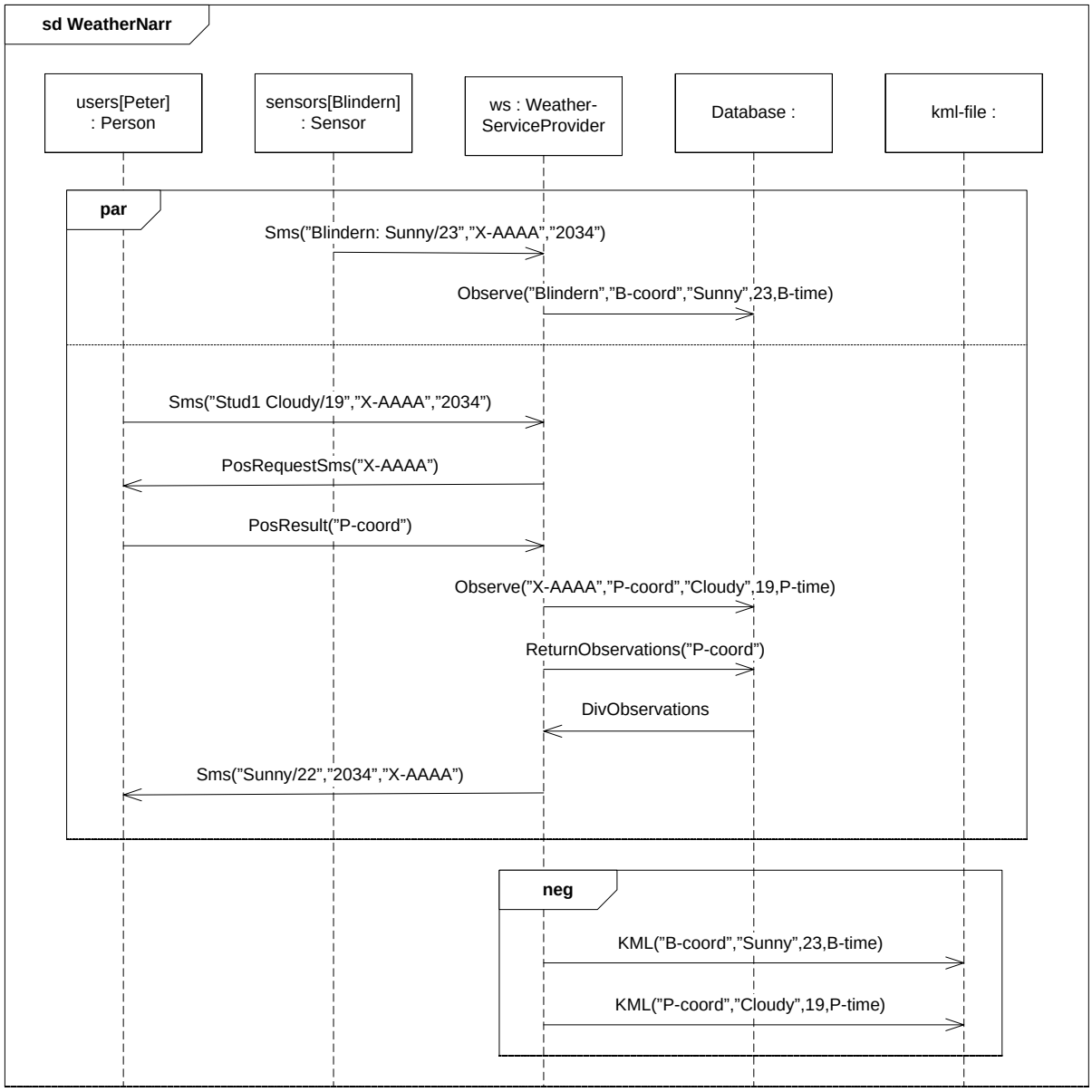
## 2 c) Refinement

I: Draw a sequence diagram that is a (pure) supplementing of the diagram in Figure 1. Explain your answer.




*The sequence diagram WeatherSupp represents a pure supplementing. By including the original diagram in one operand of the **alt** operator and specifying an entirely new trace in the other we have added a new positive trace to the interaction obligation – this is the only difference from the interaction obligation in the original specification.*

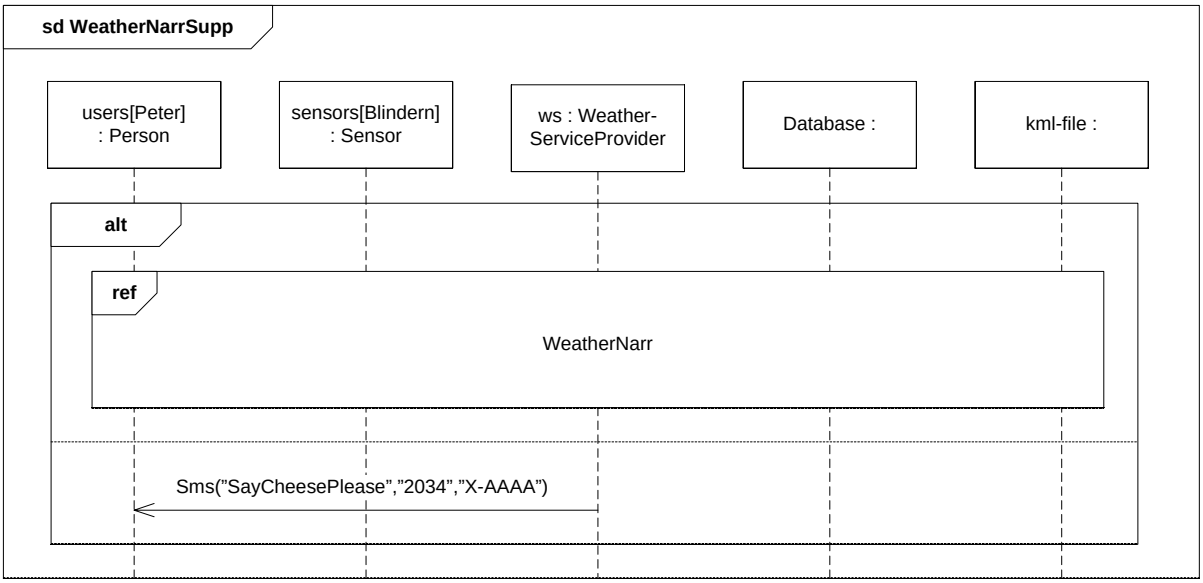
II: Draw a sequence diagram that is a (pure) narrowing of the diagram in Figure 1.




*The sequence diagram WeatherNarr represents a pure narrowing of the diagram in Figure 1. The only difference is that the **opt** operator in Weather has been replaced by a **neg** operator. This means that the traces that include the KML(...) messages are positive in the only interaction obligation in [[Weather]], but negative in the only interaction obligation in [[]WeatherNarr]].*

III: Draw a sequence diagram that fulfils all of the following requirements:

- It **is** a refinement of the diagram in Figure 1,
- It is **not** a (pure) narrowing of the diagram in Figure 1,
- It is **not** a (pure) supplementing of the diagram in Figure 1.
- It has **not** the exact same semantics as the diagram in Figure 1.




*The sequence diagram WeatherNarrSupp fulfills the stated criteria. The traces that include the KML(...) messages are positive in the original specification, but have become negative in the new specification. The trace in the second operand of the* ***alt*** *operator in WeatherNarrSupp is inconclusive in the original specification, but is positive according to WeatherNarrSupp.*

## 2 d) Refinement (continued)

Consider a sequence diagram consisting of an **xalt** where the first operand is the sequence diagram in Figure 1 and the second operand can be selected arbitrarily.
I: Is this diagram a general refinement of the diagram in Figure 1? Explain your answer.

*Yes, it is a general refinement. [[Weather]] contains only a single interaction obligation, and this interaction obligation is also contained in [[Weather* ***xalt*** *d]] for any sequence diagram d. Since every interaction obligation is a refinement of itself, it follows that the (only) interaction obligation in [[Weather]] is refined by an interaction obligation in [[Weather* ***xalt*** *d]].*

II: Is this diagram a limited refinement of the diagram in Figure 1? Explain your answer.

*In general, the answer is no. If [[d]] contains at least one interaction obligation that does not refine the (only) interaction obligation in [[Weather]], then we don't have limited refinement. This is because limited refinement requires that each interaction obligation at the concrete level (in [[Weather* ***xalt*** *d]]) is a refinement of an interaction obligation at the abstract level (in [[Weather]]).*

## *3. Risk Analysis (30%)*

The exercises below refer to the sequence diagram of Figure 1, but do not depend on what you have answered on exercises 1 and 2 above.

Assume that you are hired to conduct a security analysis on behalf of the provider of the weather service.

### 3 a) Context establishment

I: Select the most natural lifeline in the sequence diagram in Figure 1 to represent the *party (stakeholder)* of the analysis? Explain your answer.

*Since the security analysis is performed on behalf of the provider of the weather service, it is reasonable to say that the most natural lifeline to represent the party/stakeholder is ws:WeatherServiceProvider.*

II: Classify the remaining four lifelines according to whether they may be understood as *assets* or *human threats*? Explain your answer.

*All the remaining lifelines may well be understood as assets, since they contribute to the functionality of the system.*

*The users[Peter]:Person lifeline may also be understood as a human threat, since it represent a human that may harm assets, for example by sending incorrect weather information to the weather system. This can be done on purpose or by accident.*

III: Introduce an additional asset that is indirect with respect to the asset classification above.

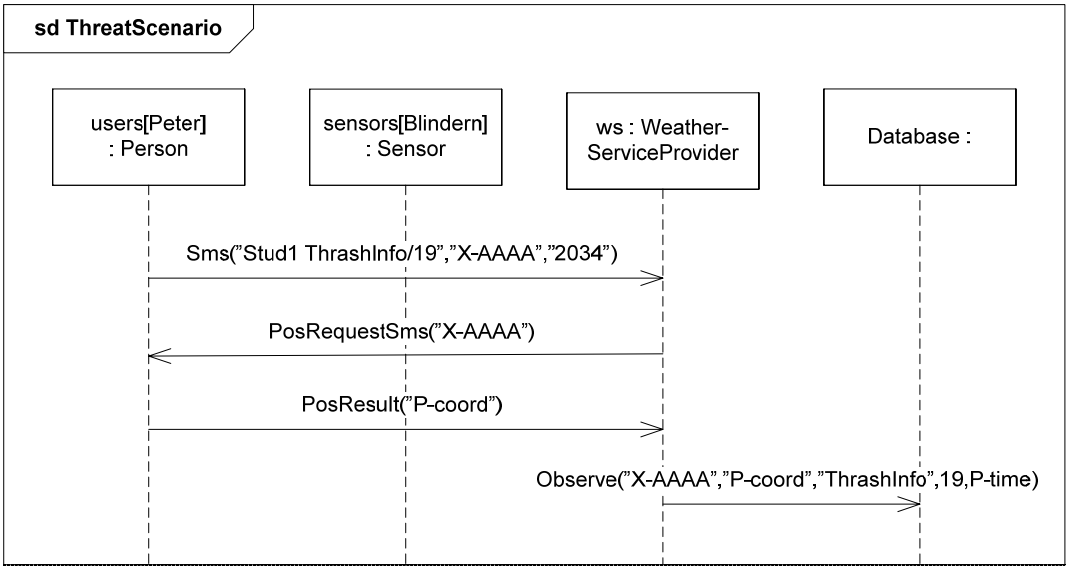
*The trust that the users have in the system is a possible indirect asset. For example, if the database is harmed then this may result in the system giving false weather information to the users, which may reduce the level of trust the users have in the system.*

### 3 b) Risk identification

Assume the service provider is particularly concerned about integrity of data. Apply the context that you have established in 3a)
I: Draw a threat diagram capturing a “threat to integrity of data in storage” scenario. Explain your diagram.


*The diagram shows the case where a saboteur sends wrong weather info to the system. The saboteur is a human that wants to harm the system. The saboteur exploits the fact that there is no control of the received information. The wrong weather info is stored in the database, and hence the integrity of the data in storage is compromised.*

II: Draw a sequence diagram that may be understood as a specialisation of the threat diagram.




## 3 c) Consequences and likelihoods

In this sub-exercise you are not obliged to talk about the weather service, but are free to make other examples and give general answers.
I: Given a threat diagram. Under what conditions does it make sense that an unwanted incident has a higher likelihood than a threat scenario pointing at it (by pointing we mean there is an arrow from the threat scenario icon to the unwanted incident icon).

*This may be the case if more than one threat scenario point to a single unwanted incident. In this case all these threat scenarios may contribute to the probability of the unwanted incident.*

II: Define a qualitative consequence scale properly (just listing values is not enough)

*Insignificant: 1-1000 NOK*
*Minor: 1001-10.000 NOK*
*Moderate: 10.001-100.000 NOK*
*Major: 100.001-1.000.000 NOK*
*Catastrophic: >1.000.000 NOK*

III: Define two different quantitative likelihood scales.

*Alternative 1 (3 step scale, by frequency)*
*Rarely: Ten times or less per decade*
*Sometimes: From 11 to 50 times per decade*
*Often: More than 50 times per decade*

*Alternative 2 (5 step scale, by probability intervals)*
*Rare: [0,0.01]*

*Unlikely:* *<0.01,0.1]*
*Possible:* *<0.1,0.3]*
*Likely:* *<0.3,0.8]*
*Almost certain:* *<0.8,1]*

IV: Why does it make sense to argue that a consequence value is "subjective" while a frequency value is "objective"?

*This makes sense because a consequence value tells how much an asset is worth for the relevant party/stakeholder, and this is up to the party/stakeholder to decide. A frequency value, on the other hand, tells how often an event occurs (or will occur) "in the real world". If different people give different frequency estimates, this means simply that one is closer to the correct answer than the other.*