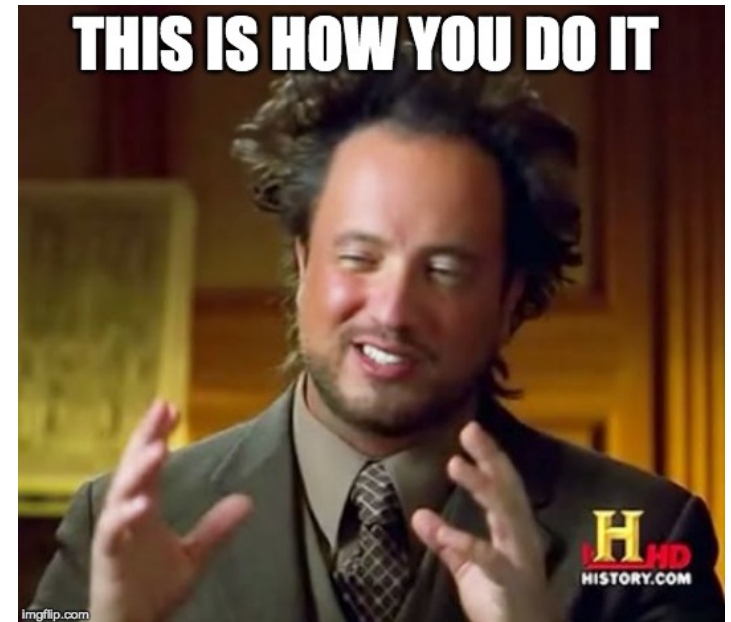


Oblig II and III (2021 ver) walkthrough

By Katrine Feten <3

Plan for this session

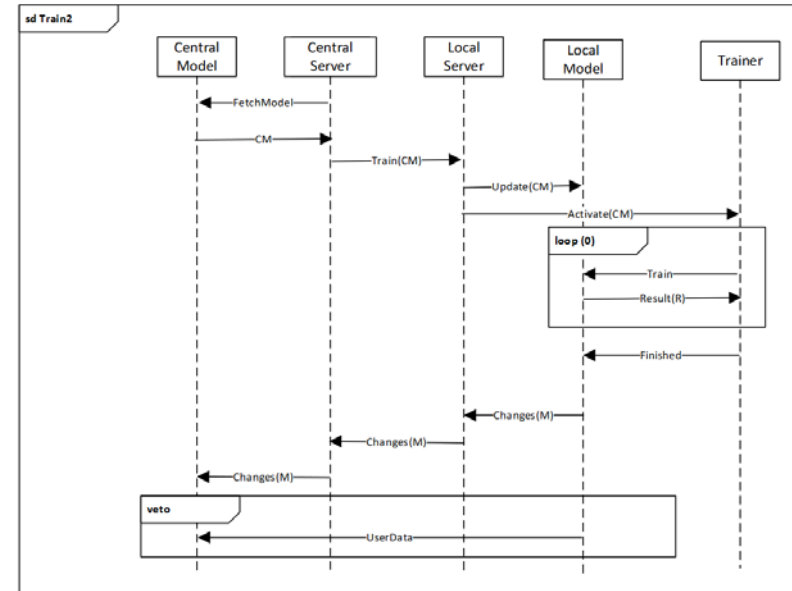
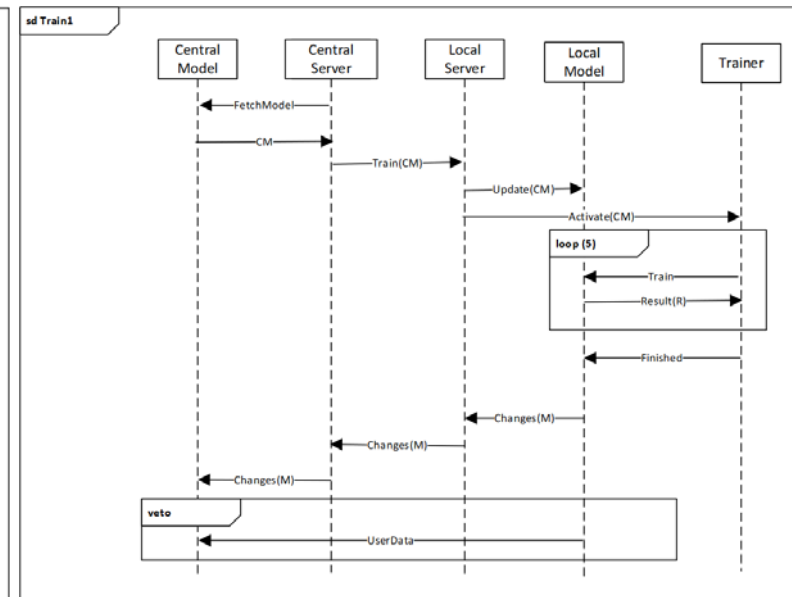
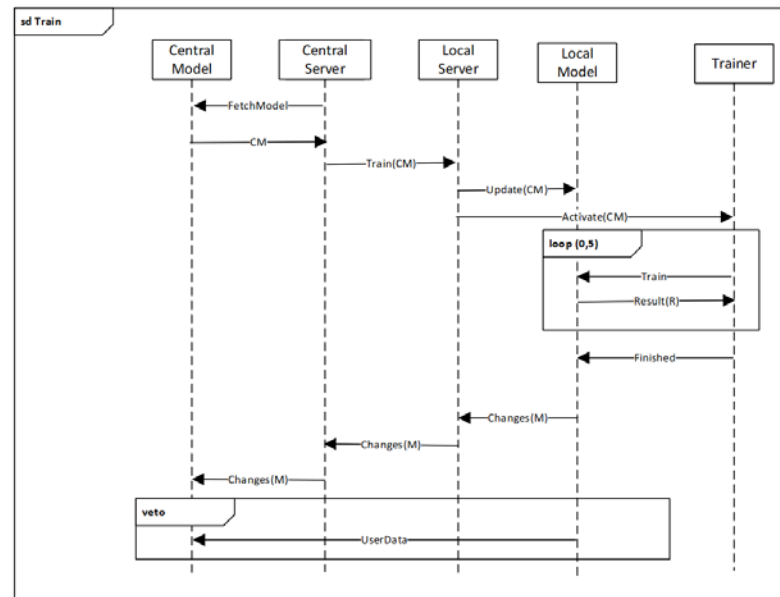
- Oblig II
 - Going through the tasks
 - Students explain
 - Solution suggestion and explanation given
- Oblig III
 - Going through the tasks
 - Students will be given 3-5 minutes to produce an answer and explain it
 - Solution suggestion and explanation given



Oblig II

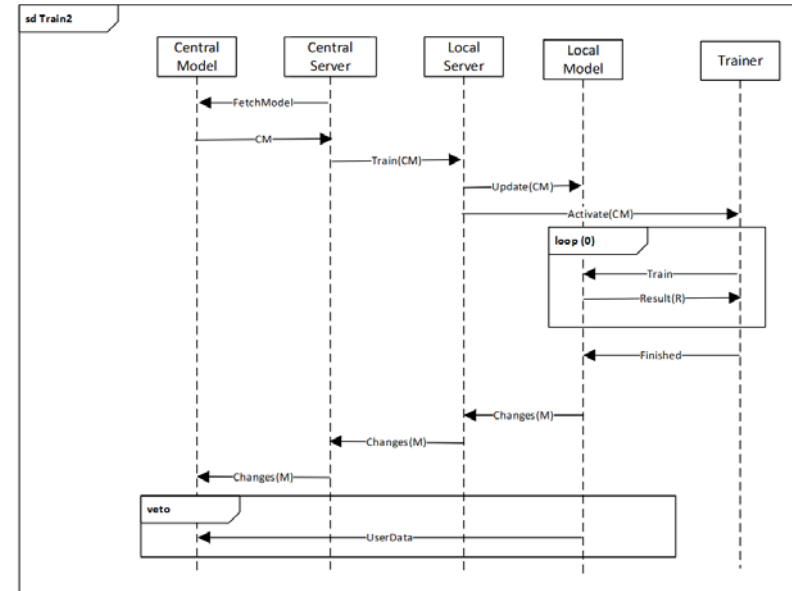
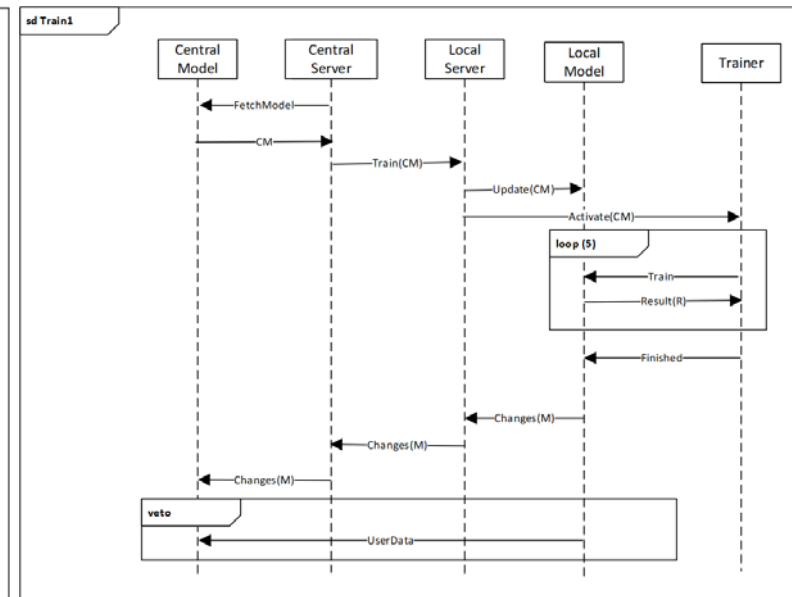
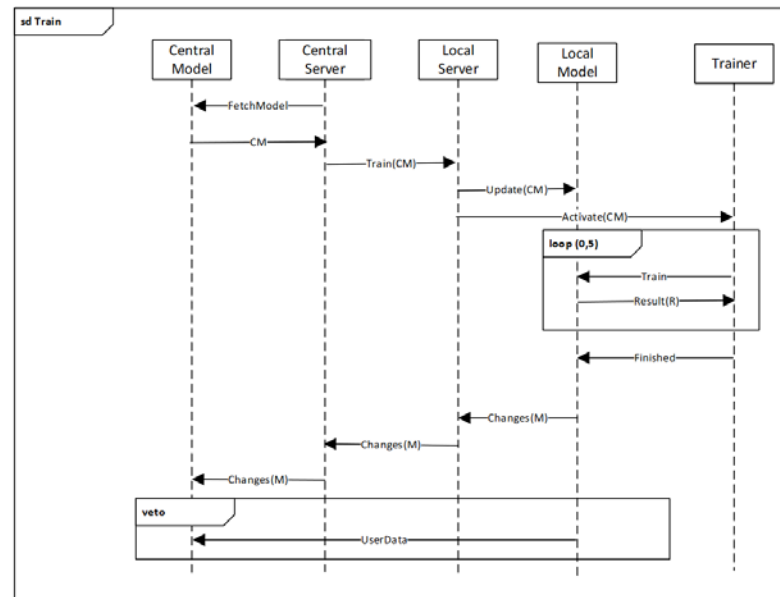
Question 1

- 1a) What is the length of the shortest positive trace described by sd Train?
Explain your answer.



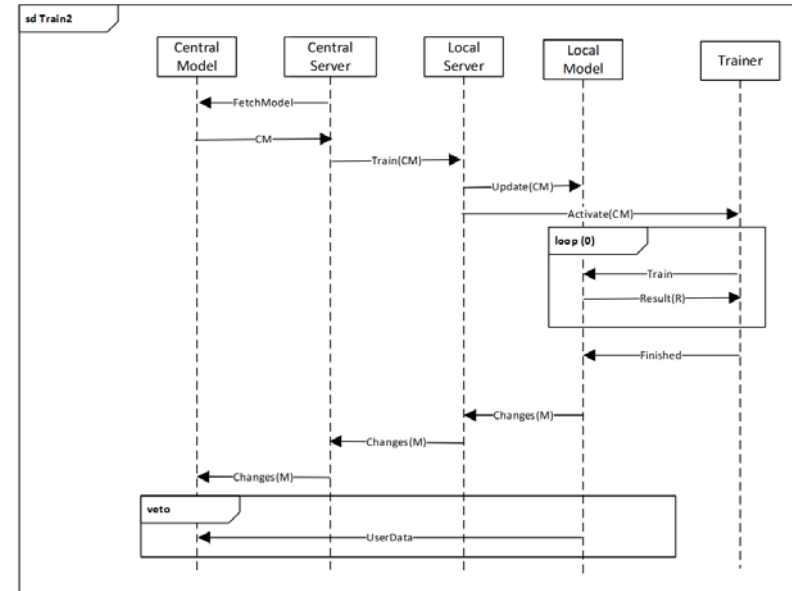
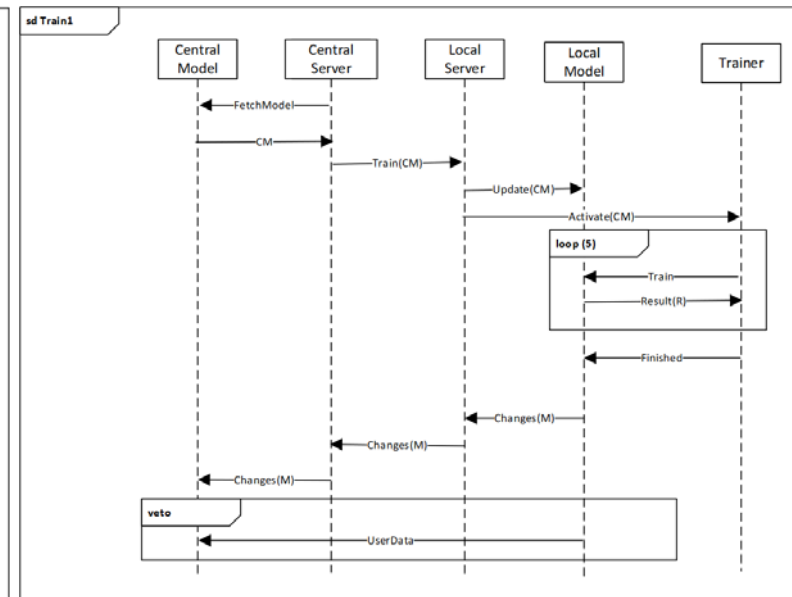
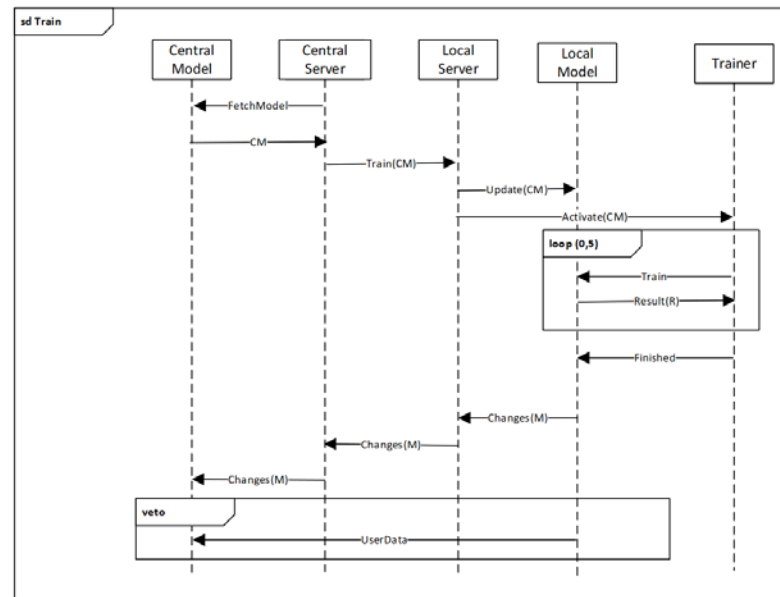
Question 1

- 1a) 18. There are 9 messages if we skip for loop and veto.



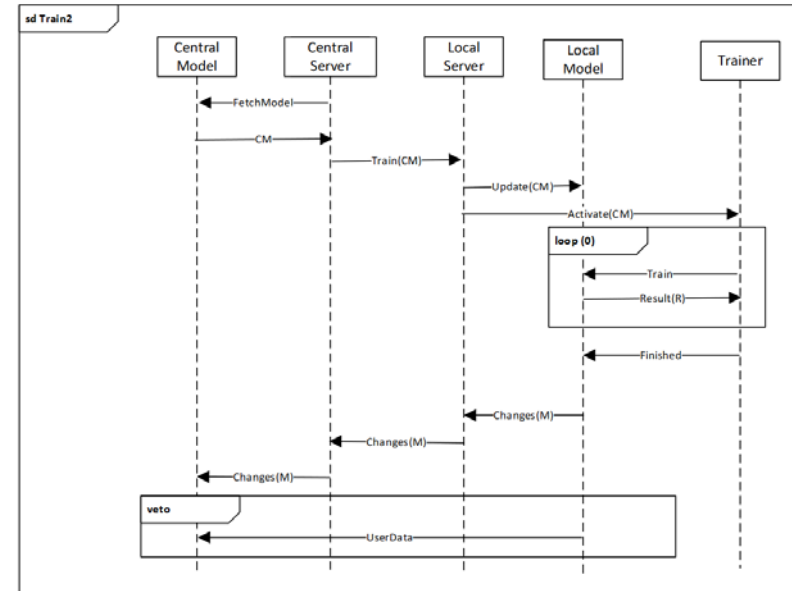
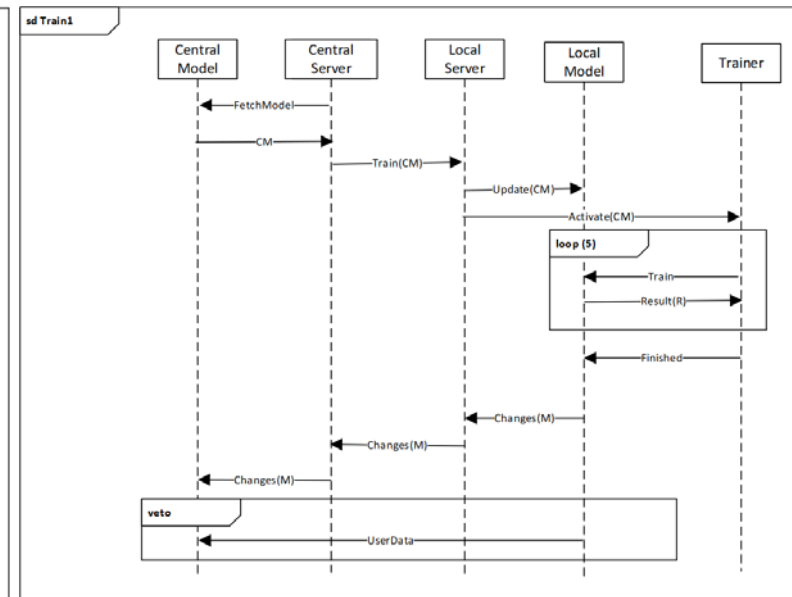
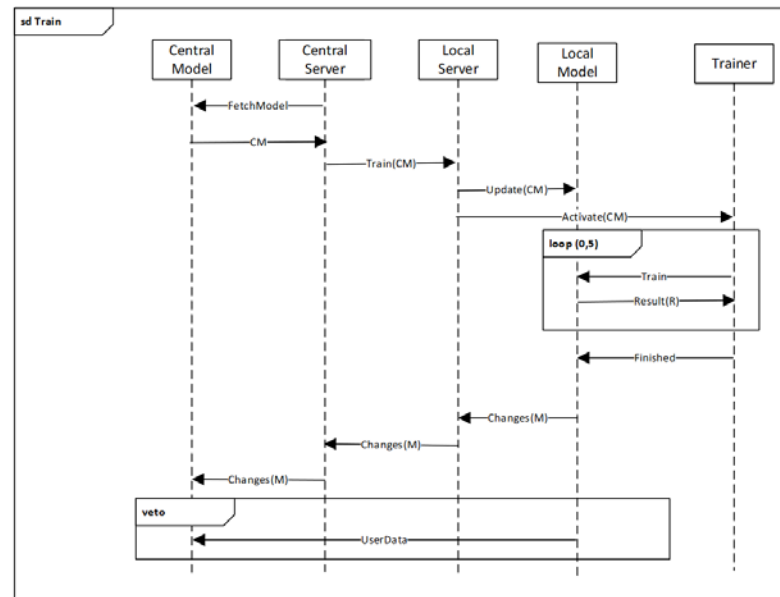
Question 1

- 1b) What is the length of the shortest negative trace described by sd Train?
Explain your answer.



Question 1

- 1b) 20. There are 10 messages if we skip for loop but execute the veto operand.

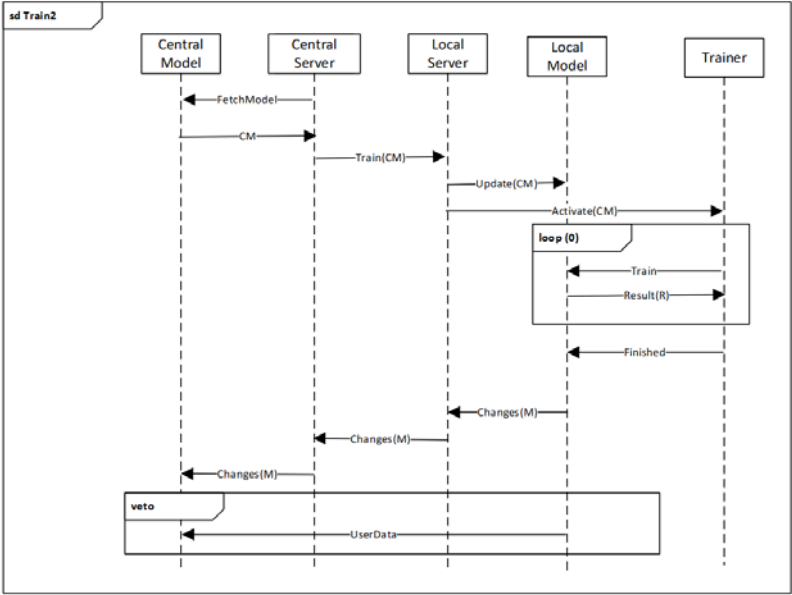
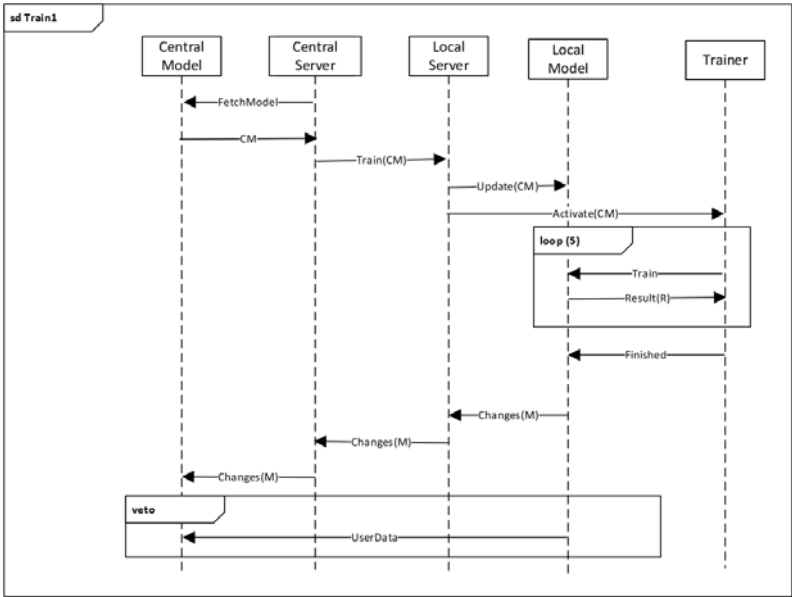
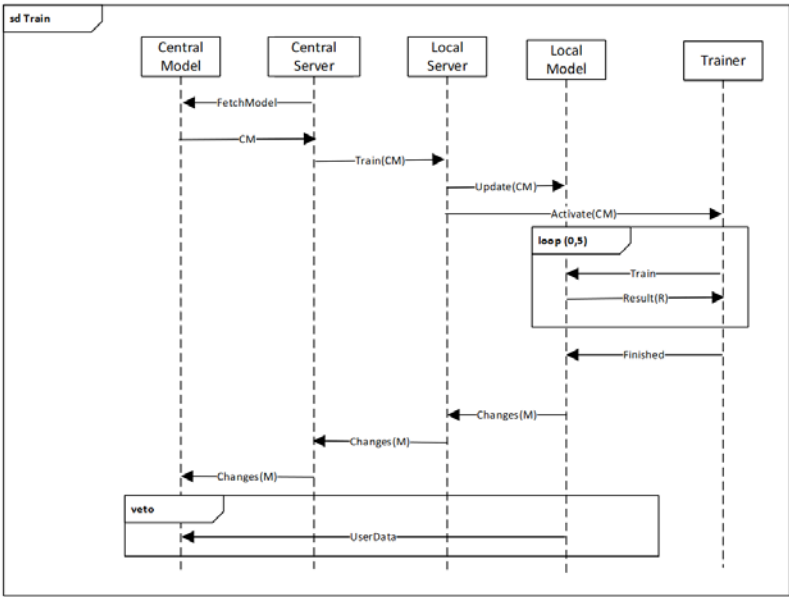


Note

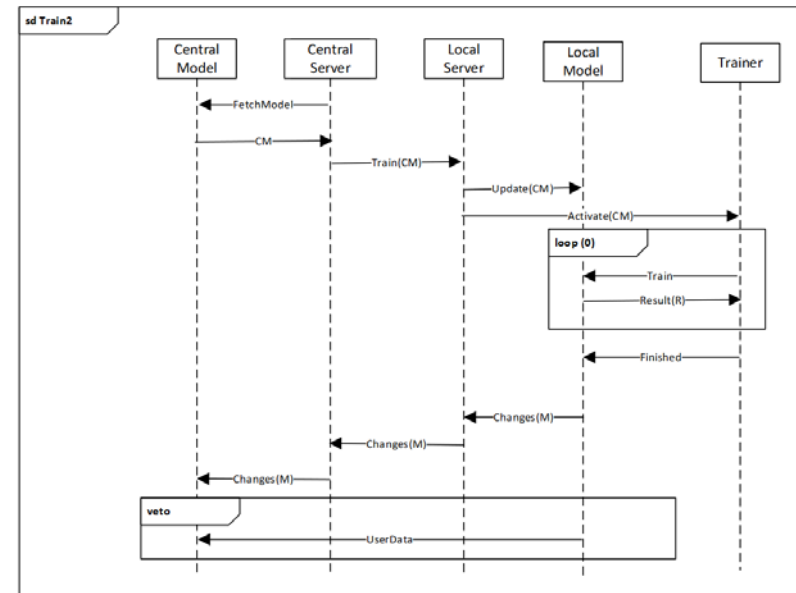
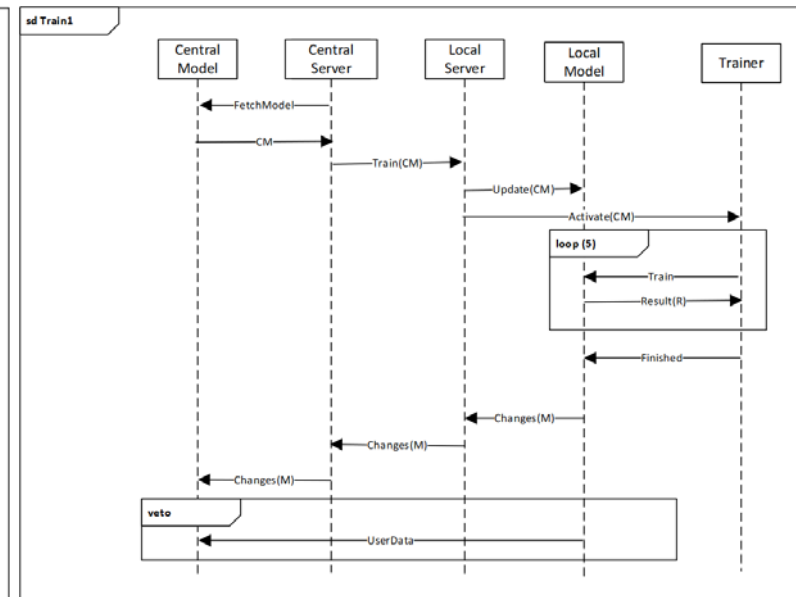
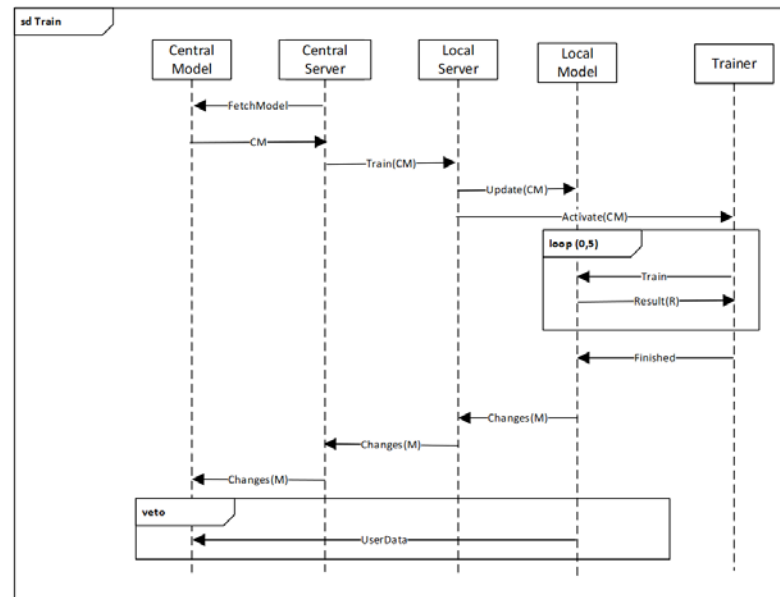
- Area of non-determinism
 - The area between two events where the ordering is undetermined
- What determines the ordering
 - The object instance lifelines
 - An event cannot be sent or received before another has been sent or arrived earlier on the lifeline

Question 1

• 1c) Assume the loop of sd Train iterates exactly five times as specified in sd Train1. How many positive traces do we get? Explain your answer.



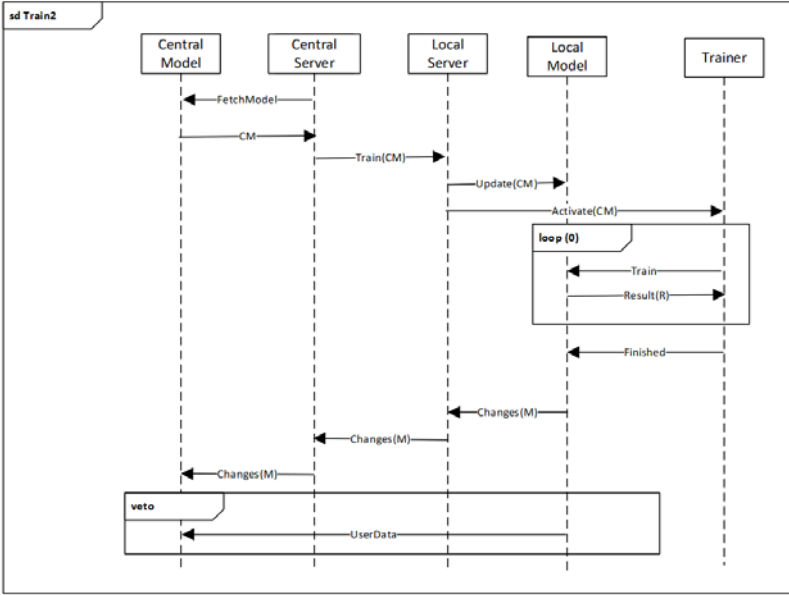
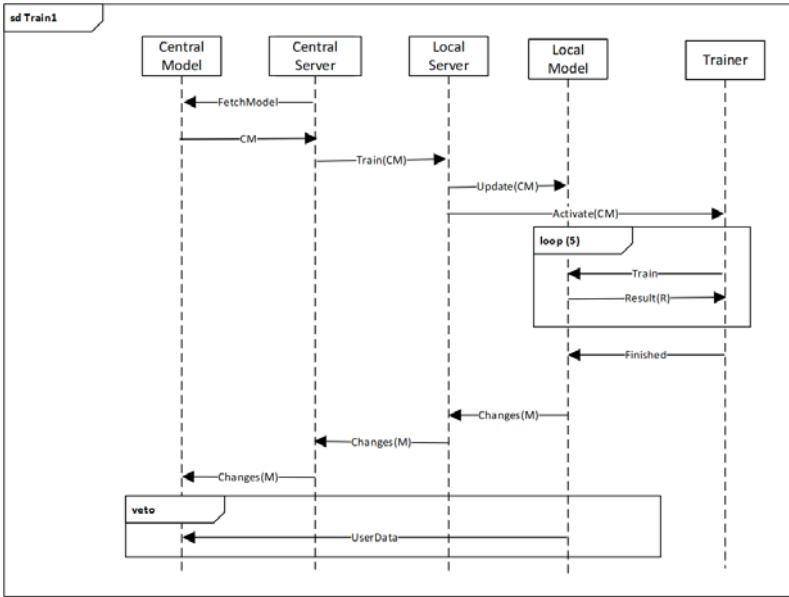
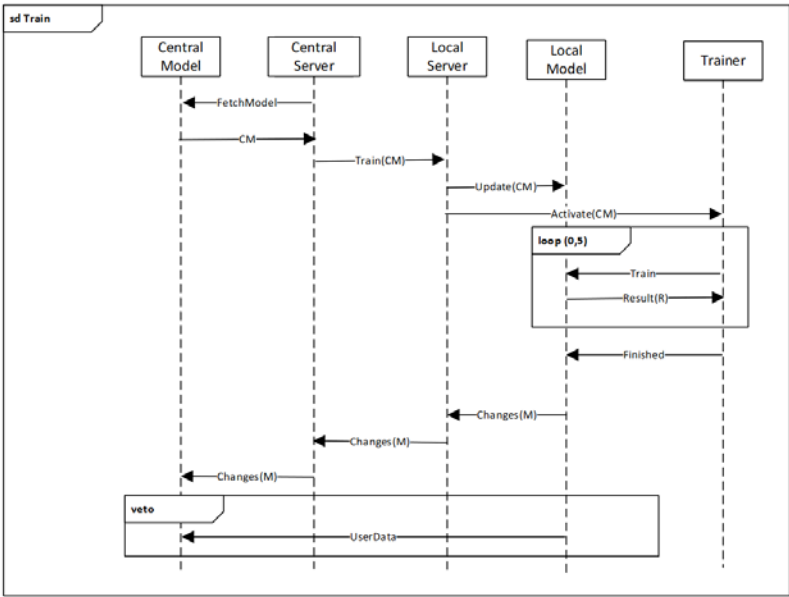
Question 1



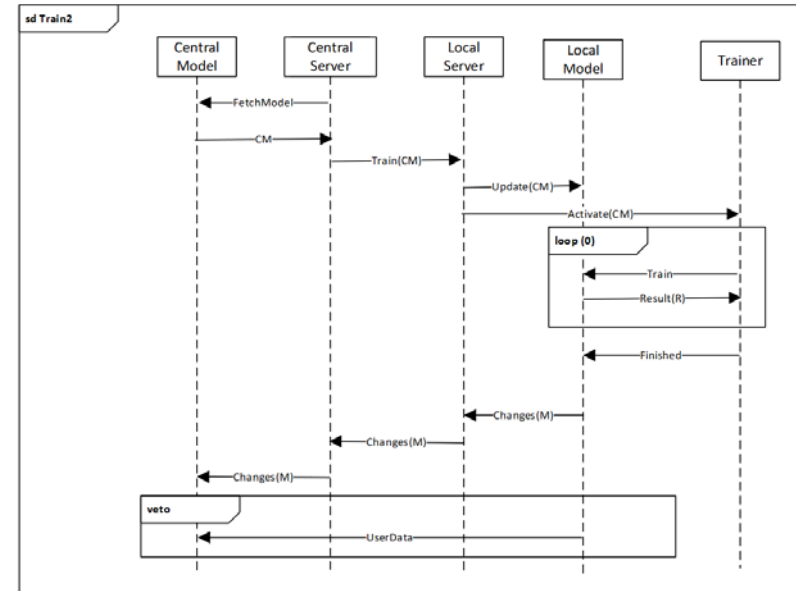
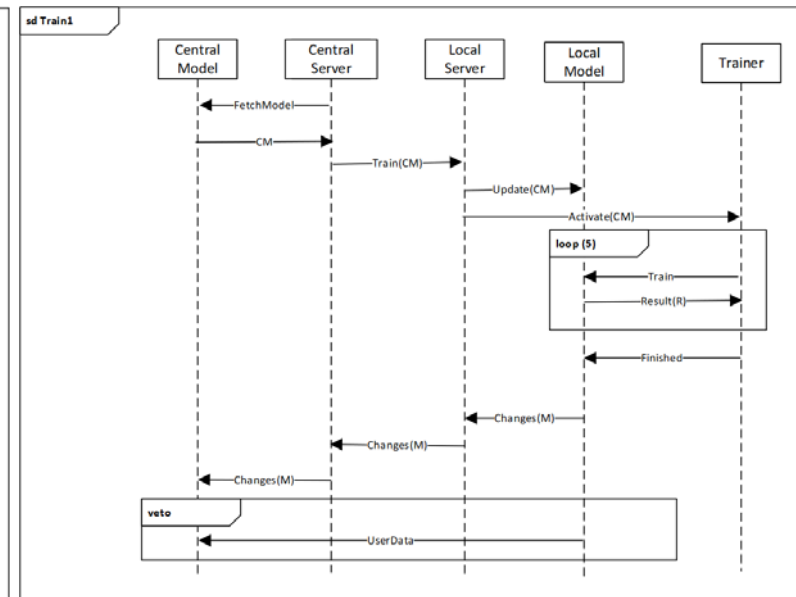
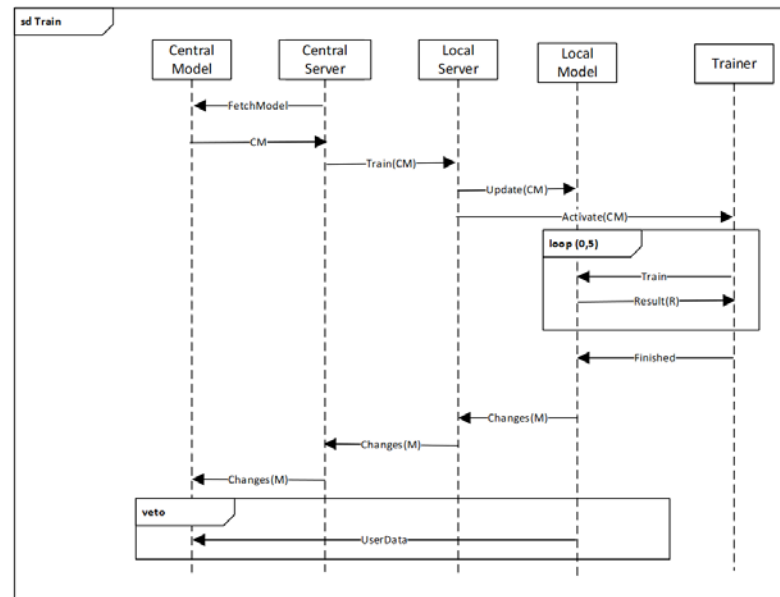
- 1c) 4. The only source of nondeterminism is ?Update(CM) that may occur anywhere in between <!Update(CM), !Activate(CM), ?Activate(CM), !Train, ?Train>

Question 1

• 1d) Assume the loop of sd Train iterates exactly zero times as specified in sd Train2. How many negative traces do we get? Explain your answer.



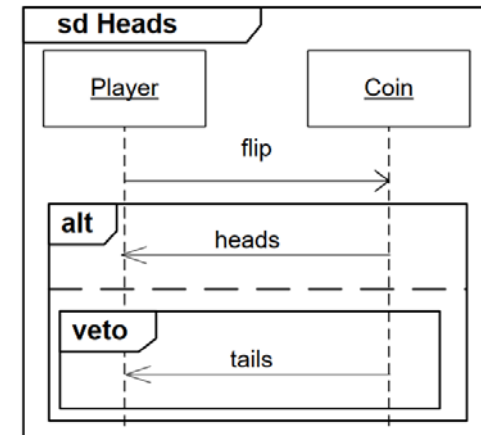
Question 1



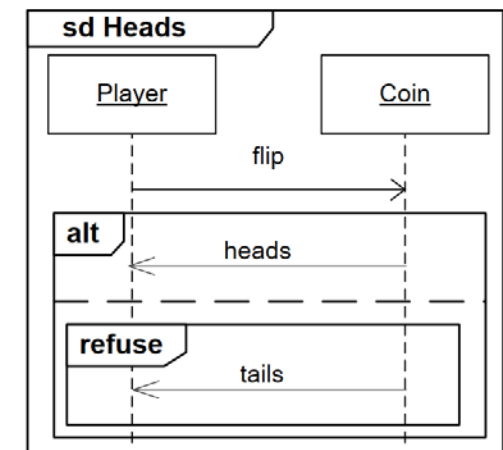
- 1d) 24. There are two sources of nondeterminism
 - ?Update(CM) that may occur anywhere in between $\langle !\text{Update(CM)}, !\text{Activate(CM)}, ?\text{Activate(CM)}, !\text{Finished}, ?\text{Finished} \rangle$
 - !UserData that may occur anywhere in between $\langle !\text{Changes(M)}, ?\text{Changes(M)}, !\text{Changes(M)}, ?\text{Changes(M)}, !\text{Changes(M)}, ?\text{Changes(M)}, ?\text{UserData} \rangle$

Note

- Veto vs refuse when positive
 - Veto: $\{<>, <!, ?>\}$ <- empty trace
 - Refuse: $\{, <!, ?>\}$ <- no trace
- Refuse is used for alts
- Example:
 - Veto gives two positive traces, and one negative
 - Refuse gives one positive, and one negative



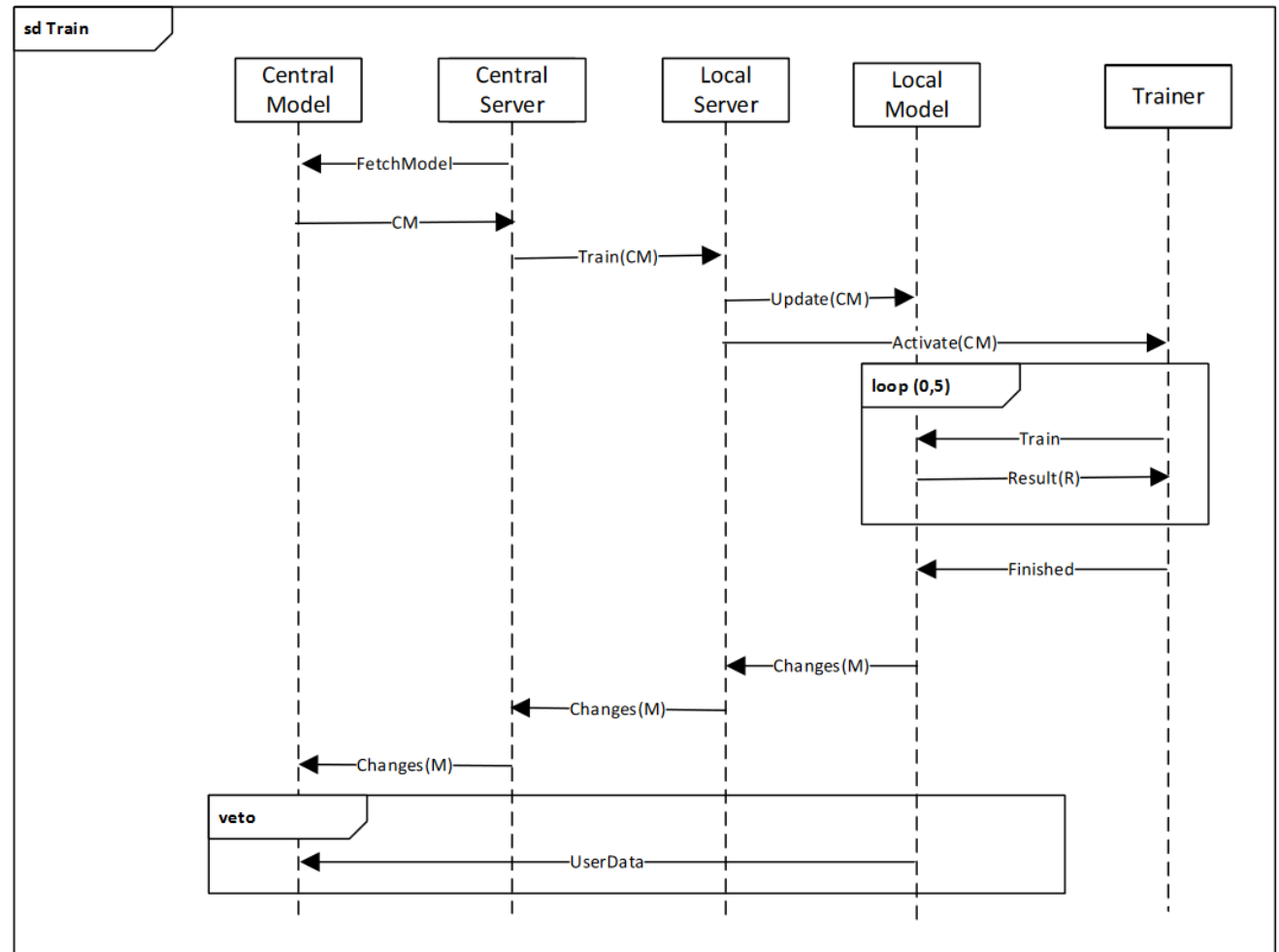
$[[\text{Heads}]] = \{(\{<!f, ?f, !h, ?h>, <!f, ?f>\}, \{<!f, ?f, !t, ?t>\})\}$



$[[\text{Heads}]] = \{(\{<!f, ?f, !h, ?h>\}, \{<!f, ?f, !t, ?t>\})\}$

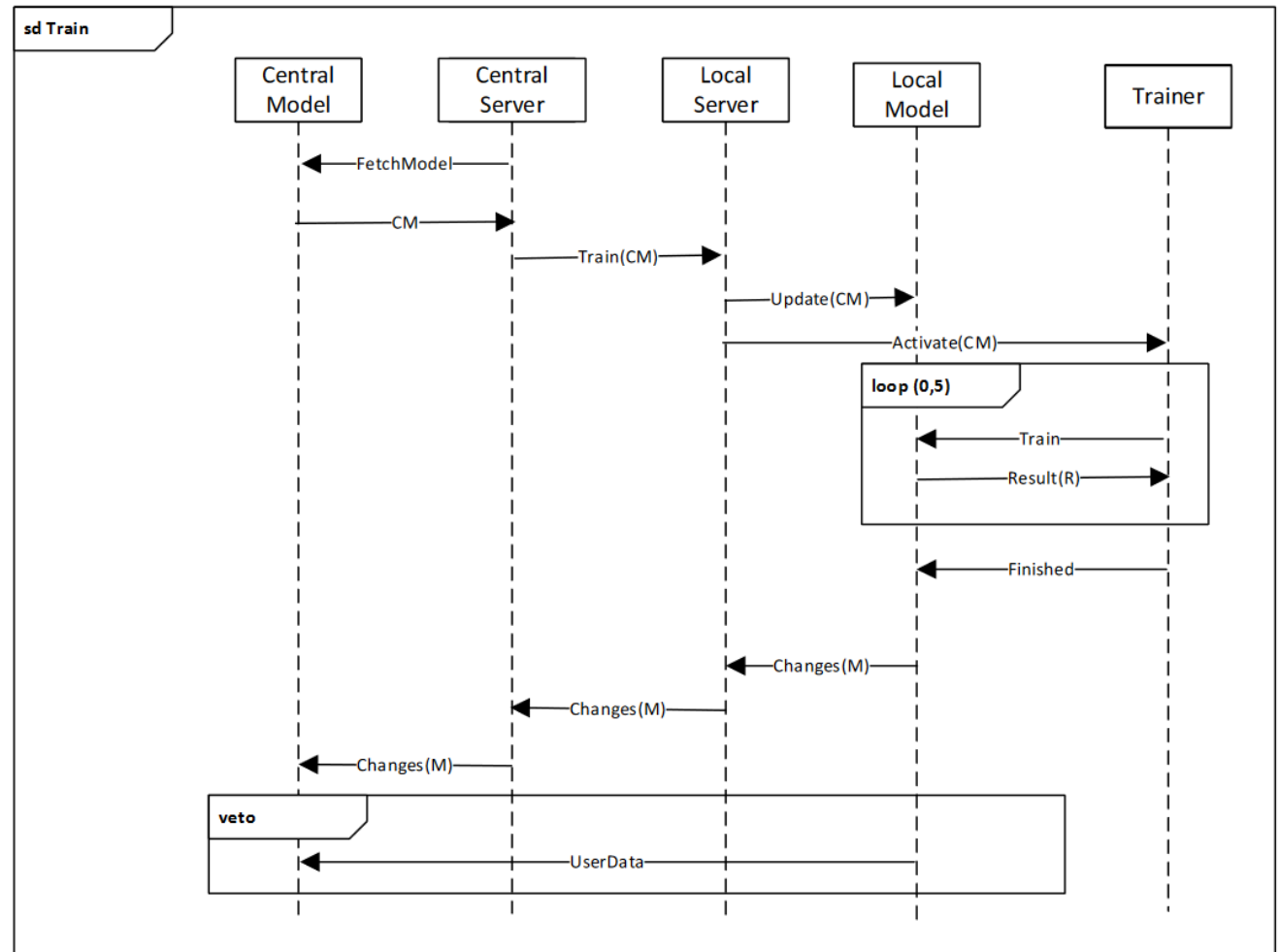
Question 2

- 2a) Explain how to change sd Train into a sequence diagram sd Train3 with no veto construct so that sd Train3 and sd Train have identical semantics.



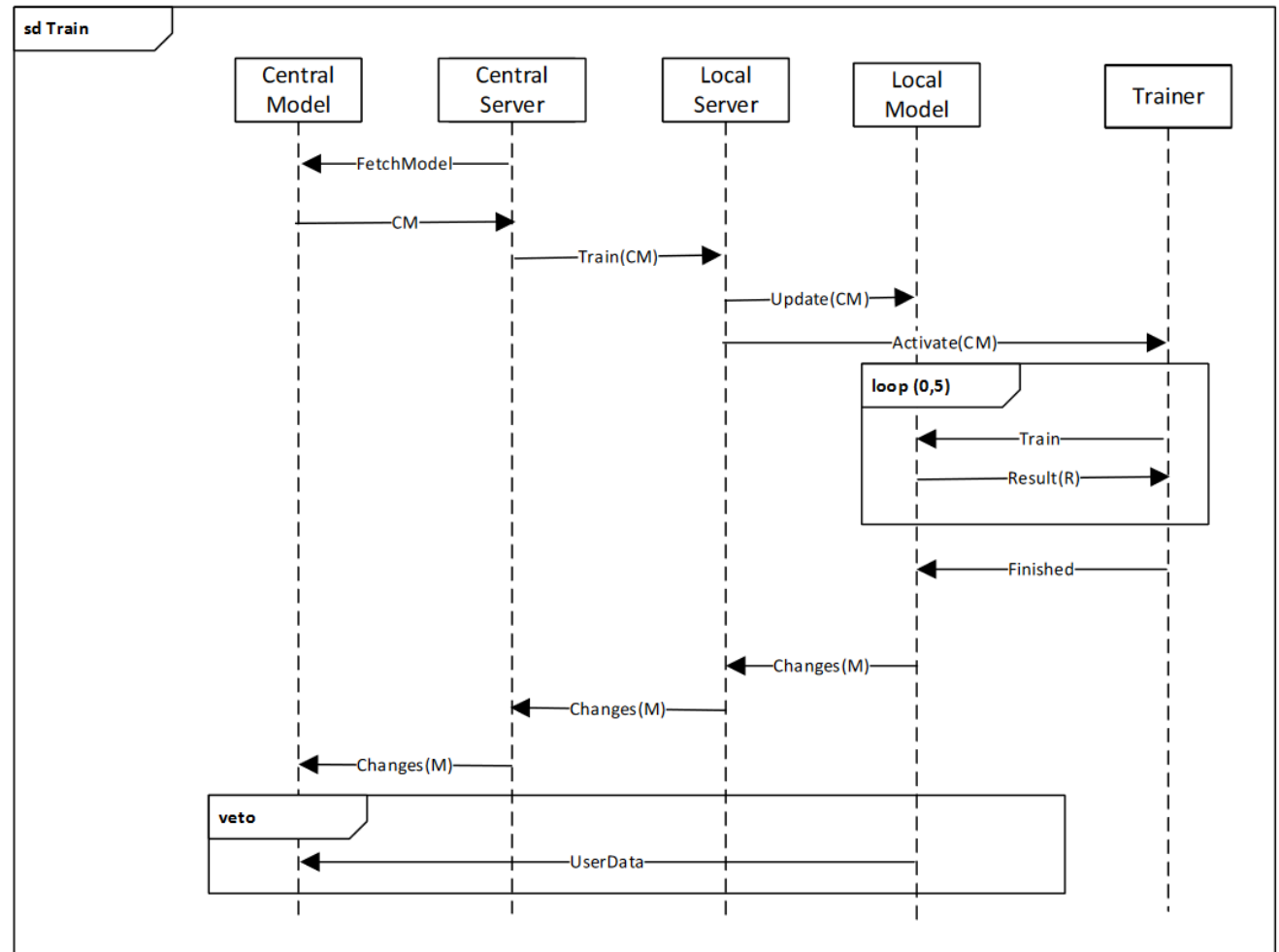
Question 2

- 2a) Use alt with two operands as the main construct of sd Main3.
 - Put everything above the veto in sd Main into the first operand.
 - Use refuse as the main construct in the second operand. It should contain everything above the veto in sd Main and the veto operand (but not the veto operator)
- This is just an example, many found the right answer another way.



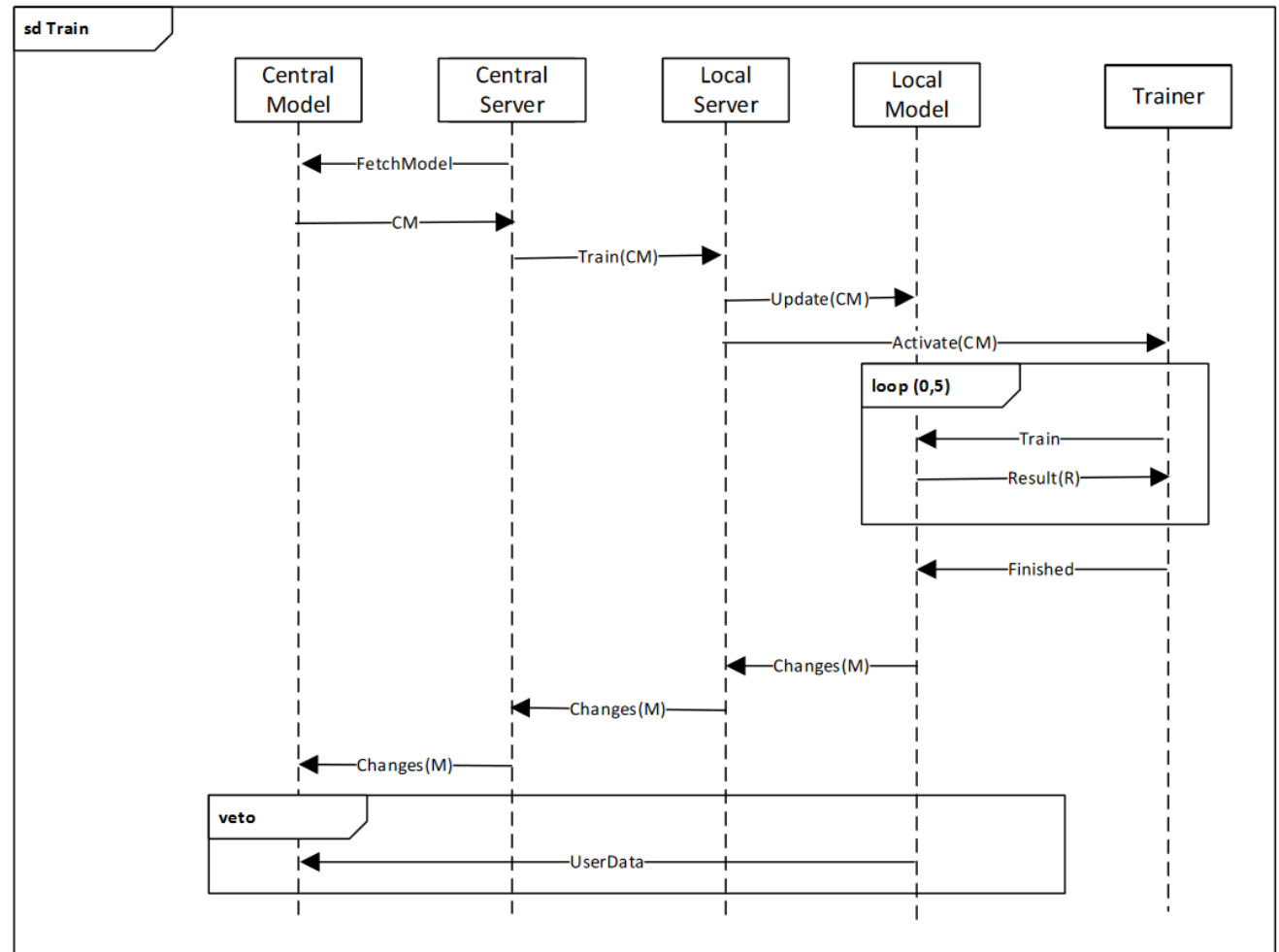
Question 2

- 2b) Explain how to change sd Train into a sequence diagram sd Train4 with no loop construct so that sd Train4 and sd Train have identical semantics.

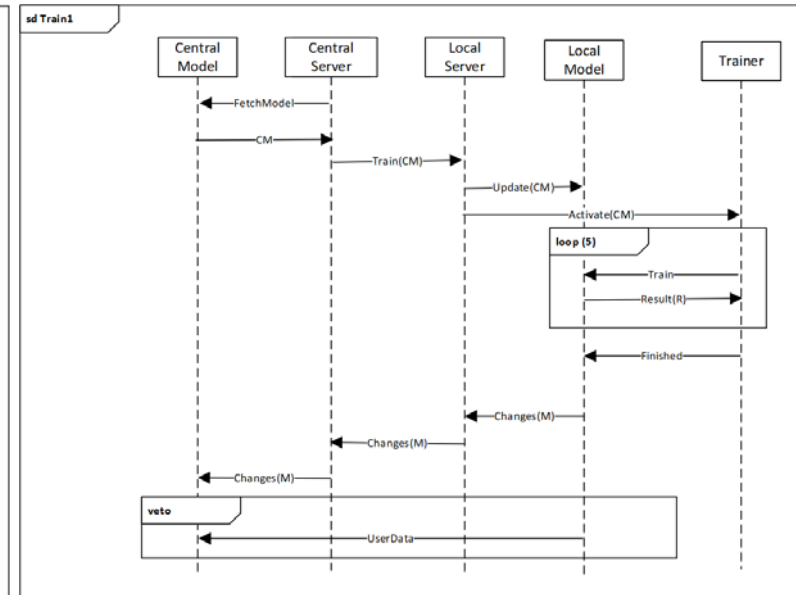
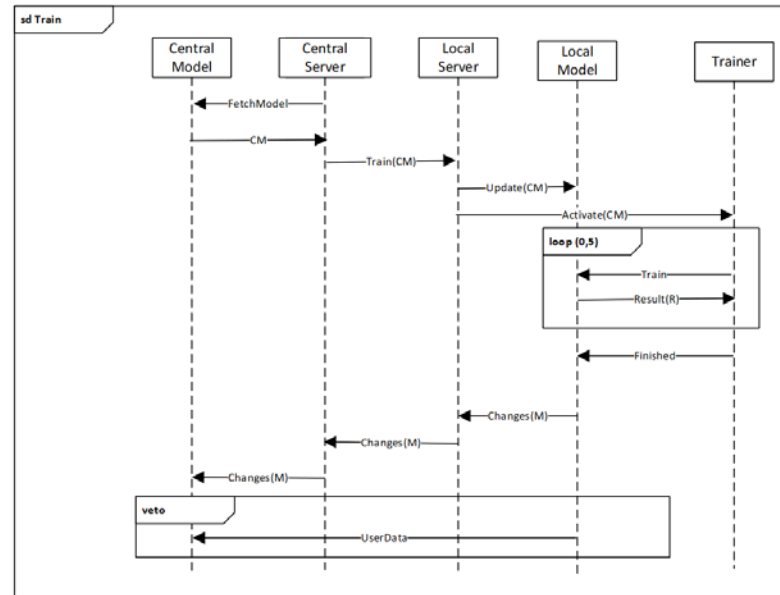


Question 2

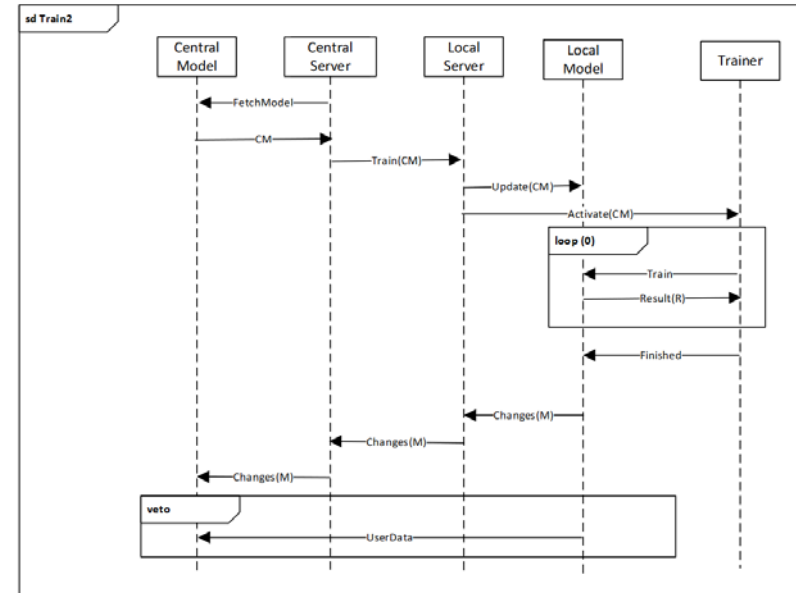
- 2b) Transform Train into Train4 by replacing the loop construct in Main with an alt construct with five operands.
 - Use the opt construct as the main construct in the first operand. Use the operand of the loop in sd Main as the operand of the opt.
 - In the other four operands of the alt construct repeat the operand of the loop two, three, four and five times respectively.
- This is also just an example.



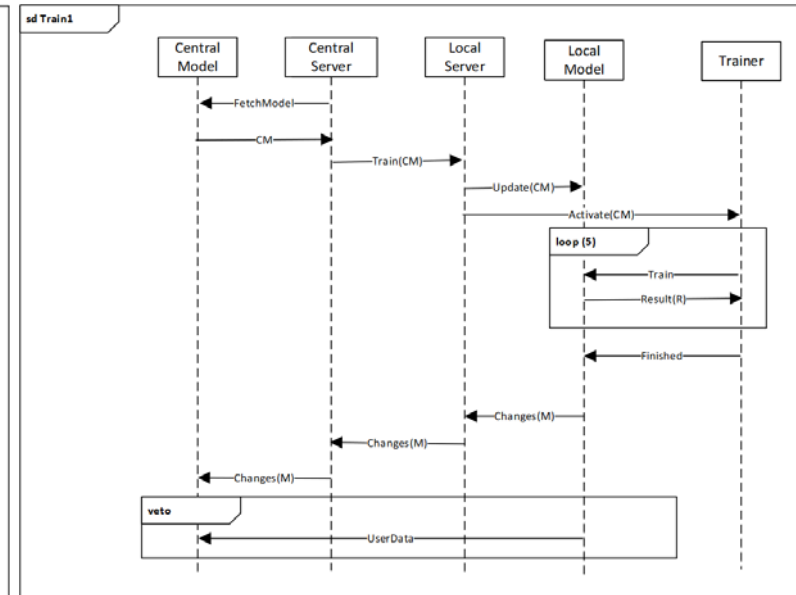
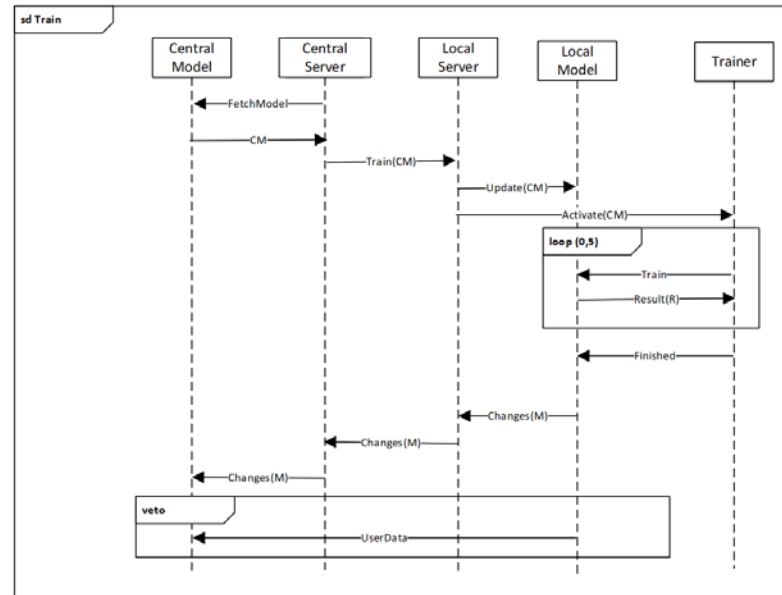
Question 2



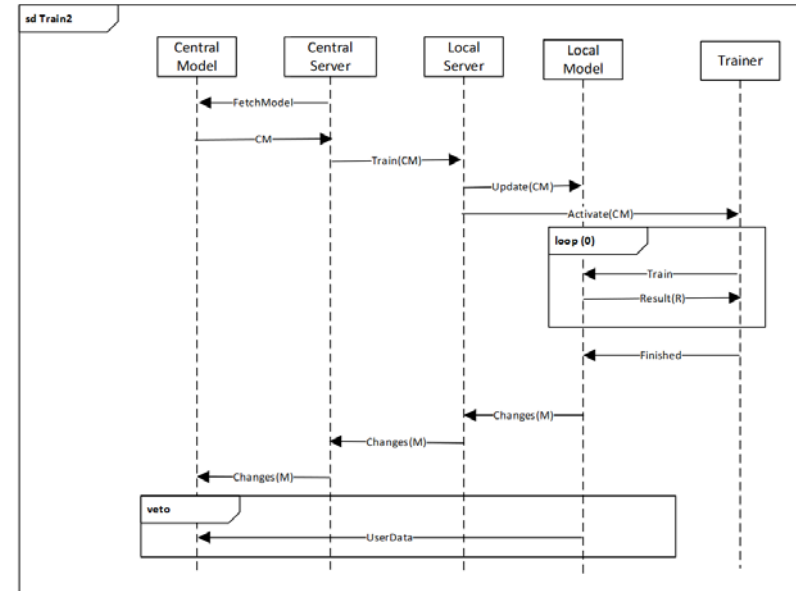
- 2c) Explain to what extent any pair of Train, Train1 and Train2 as presented in Question 1 can be related by refinement?



Question 2



- 2c) Train1 and Train2 both have traces that are inconclusive in the other. Hence, they do not refine each other. However, any positive/negative trace in Train1/Train2 is positive/negative in Train. Hence, Train supplements both Train1 and Train2.

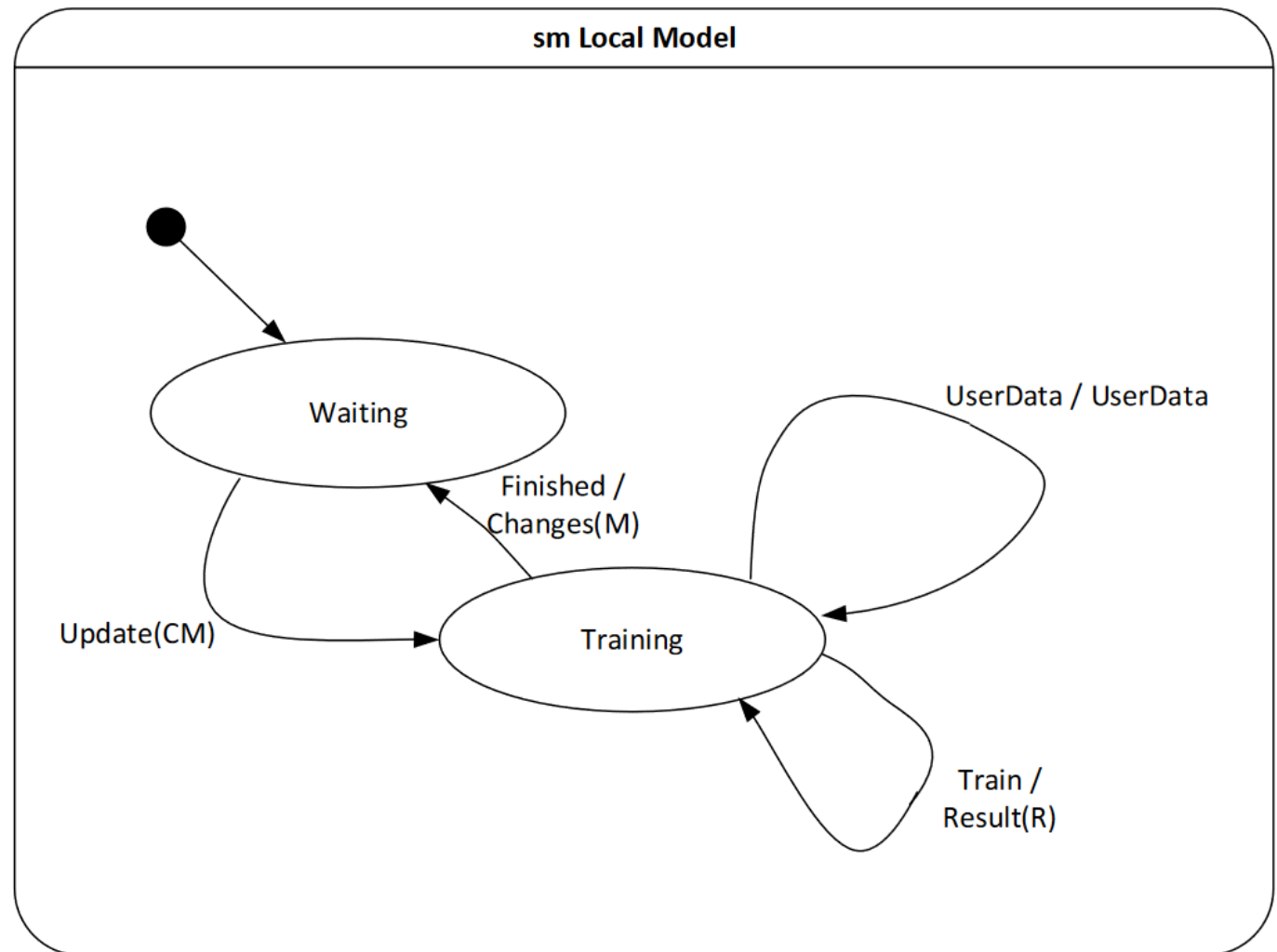


Note

- What is the one big difference between a sequence diagram and a state machine?
 - A sequence diagram shows the interactions between instances of an object/module for a given use case
 - A state machine **shows all possible interactions** with a given module
 - Thus, a state machine is interactive/responsive, it does not initialize
- What does this mean for traces?
 - A sequence diagram shows all messages sent and received, thus
 - <!receive, **?receive**, **!send**, ?send, > <- send-receive format, initialization
 - A state machine only shows what it **receives and sends**, thus
 - Receive/Send <- Receive, /Send <- interact, response
 - **<?receive, !send>**

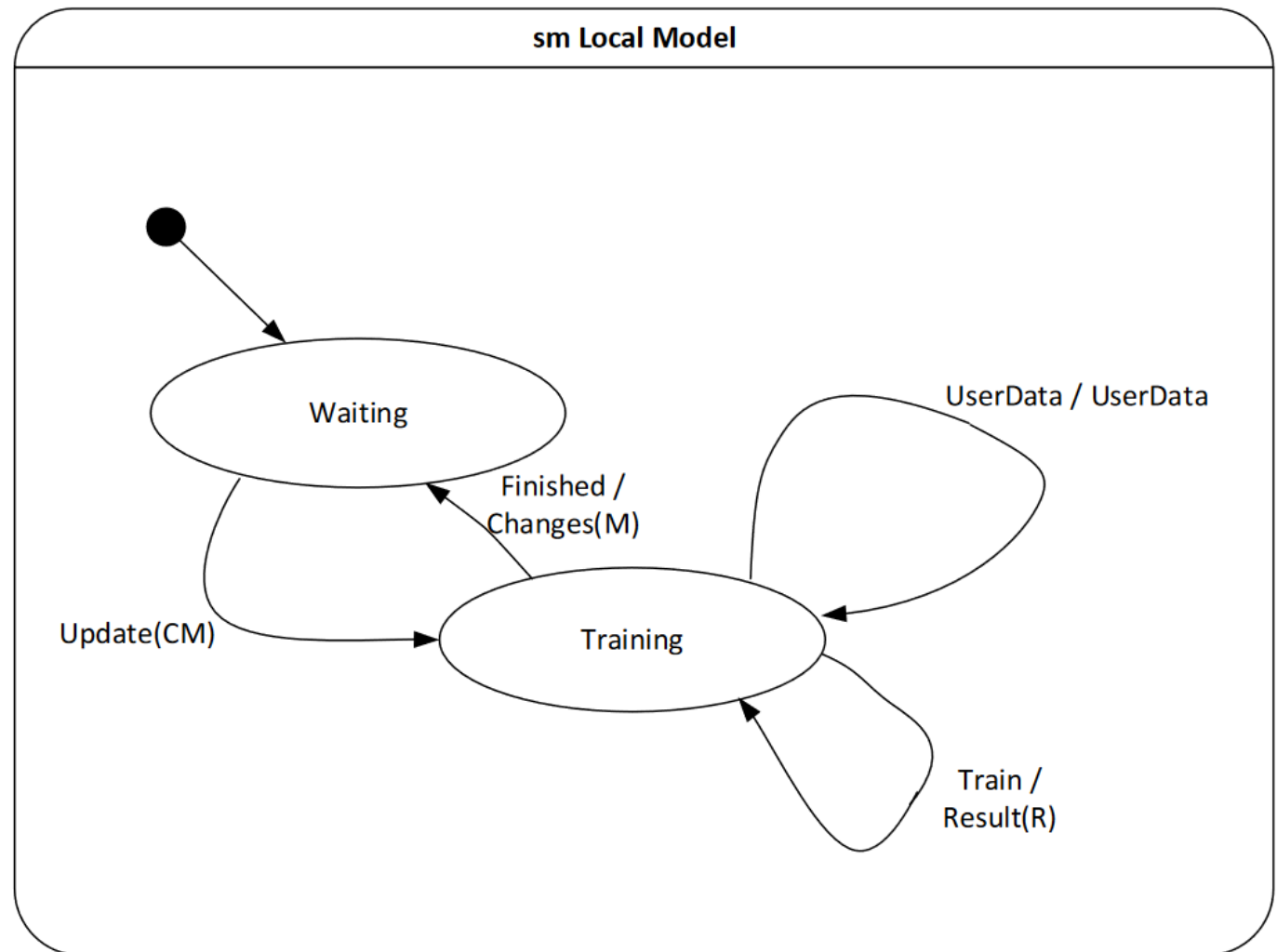
Question 3

- 3a) Describe one positive trace of sm Local Model.



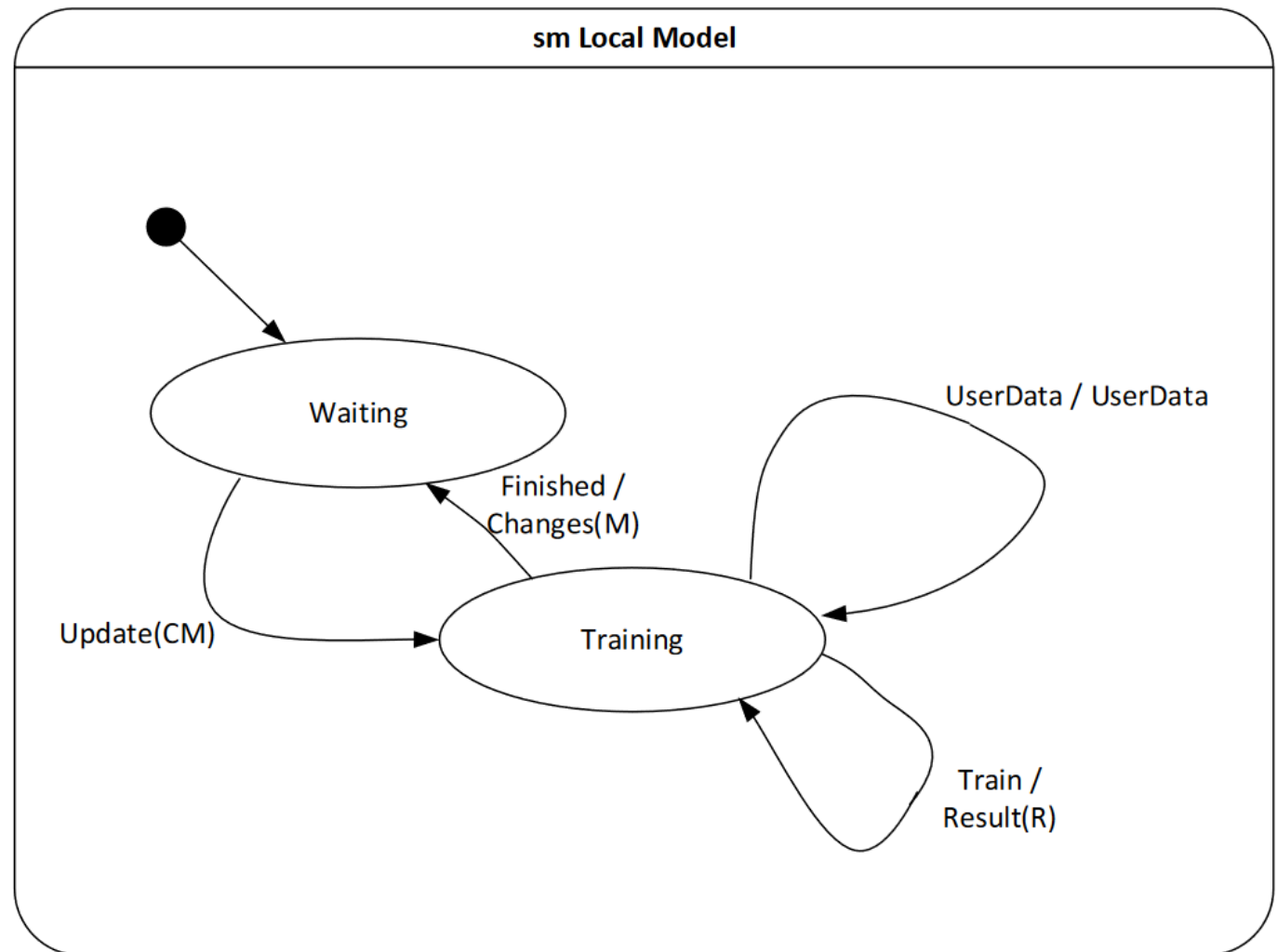
Question 3

- 3a) $\leftrightarrow$ if no input is ever received, as an example.



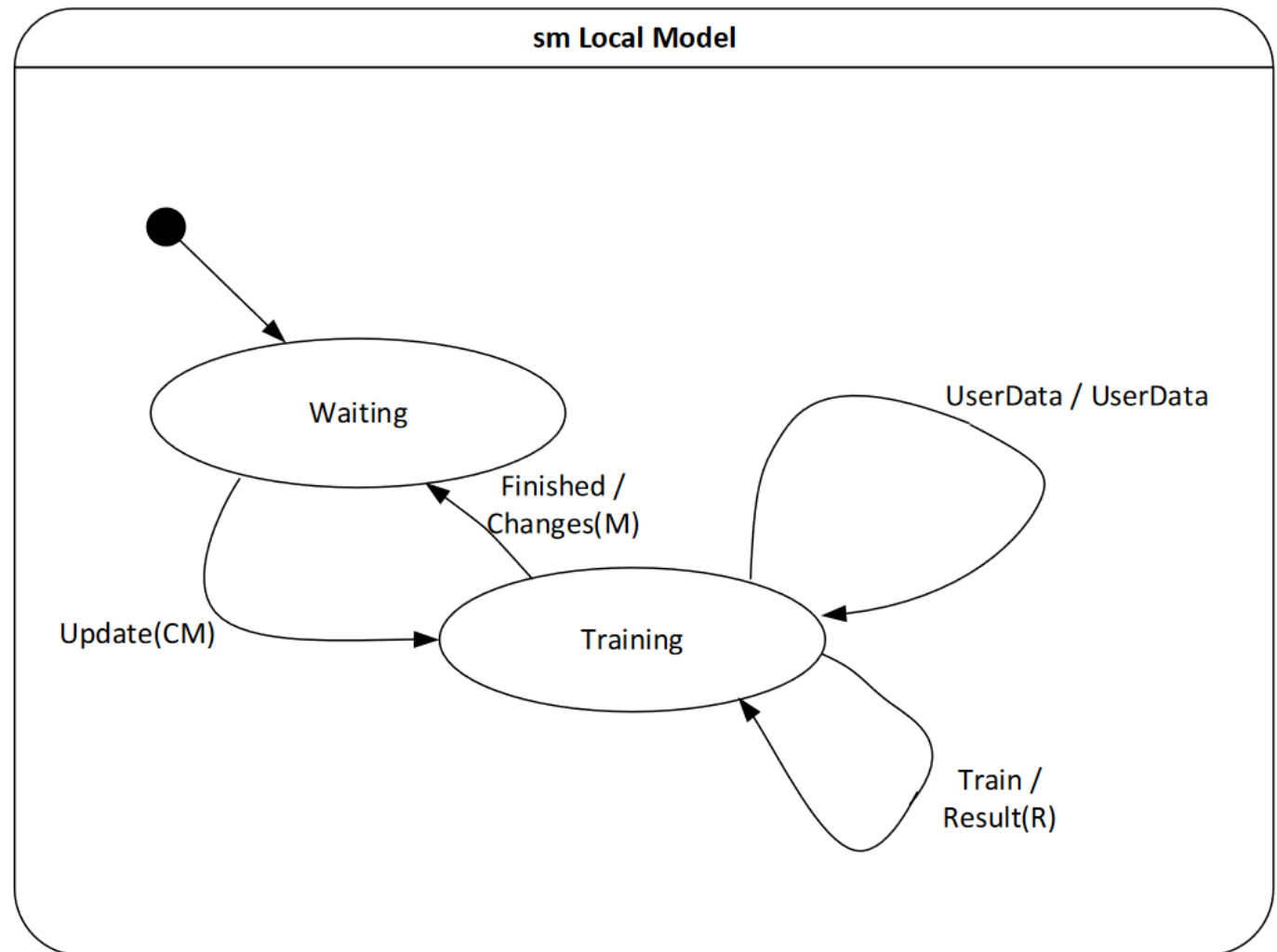
Question 3

- 3b) Describe one negative trace of sm Local Model.



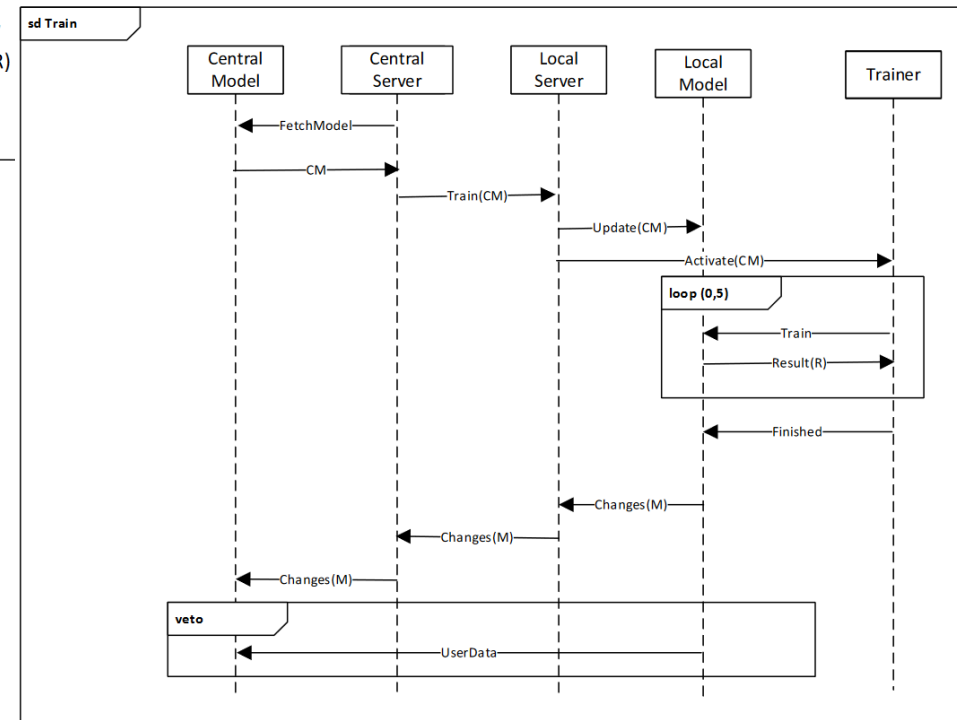
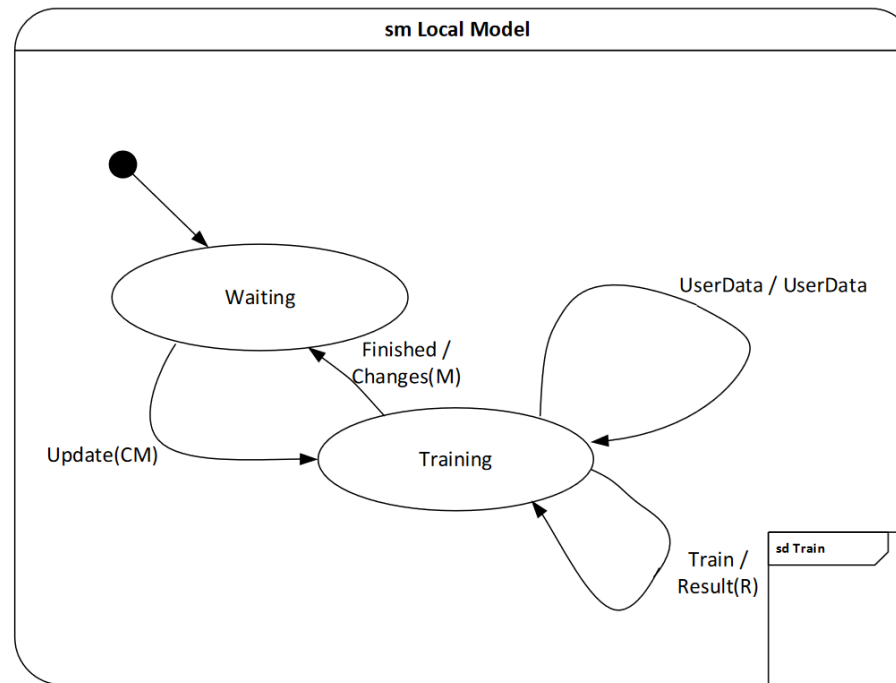
Question 3

- 3b) Any trace of length 2 whose first event is ?Update(CM) and whose second event is an output event is negative.

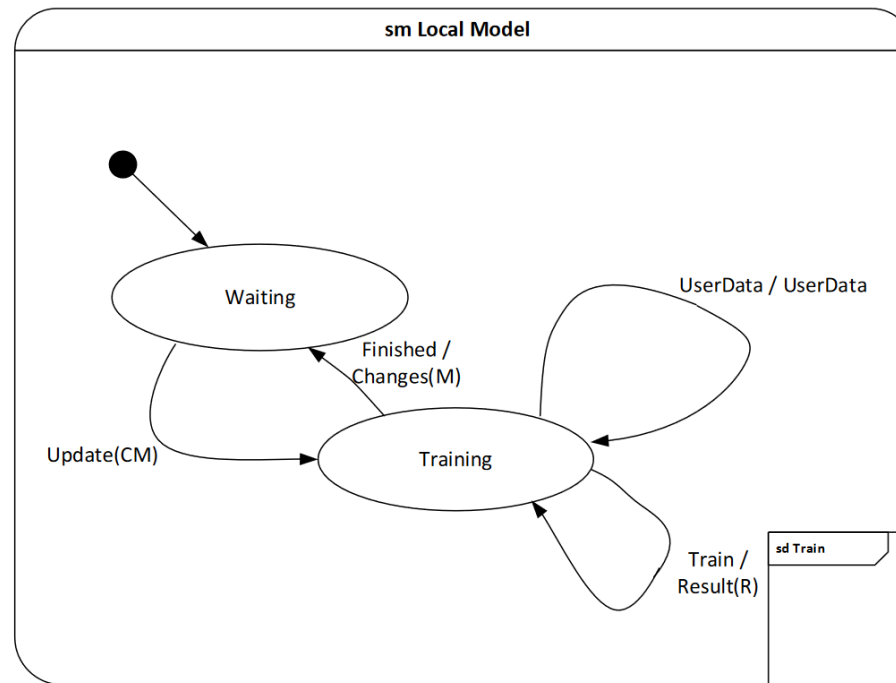


Question 3

- 3c) Is sm Local Model consistent with the lifeline Local Model in sd Train? Explain your answer.

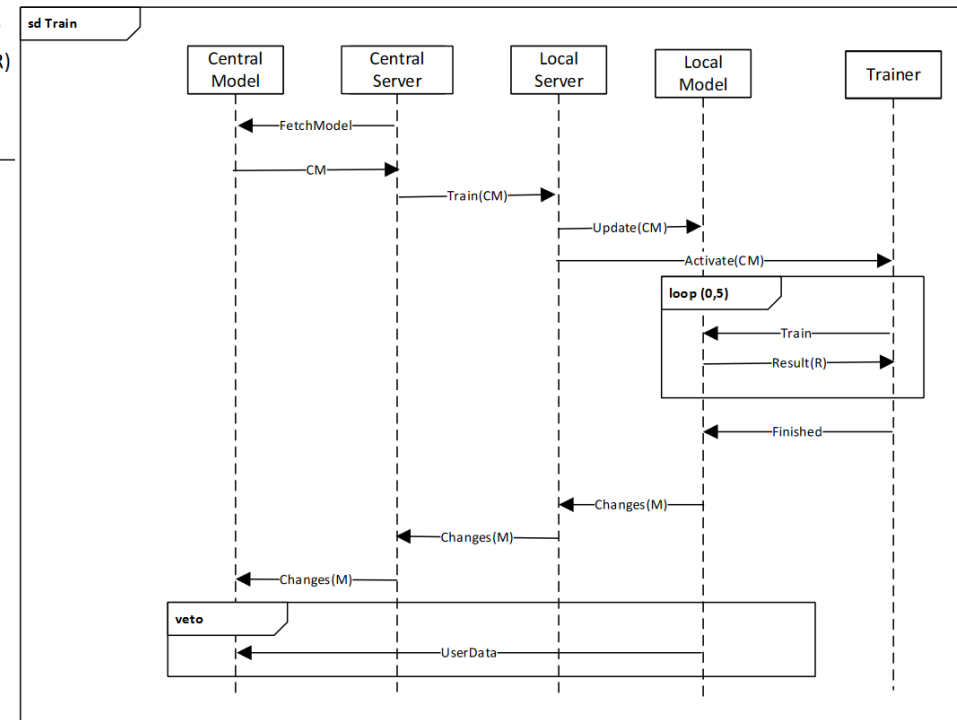


Question 3

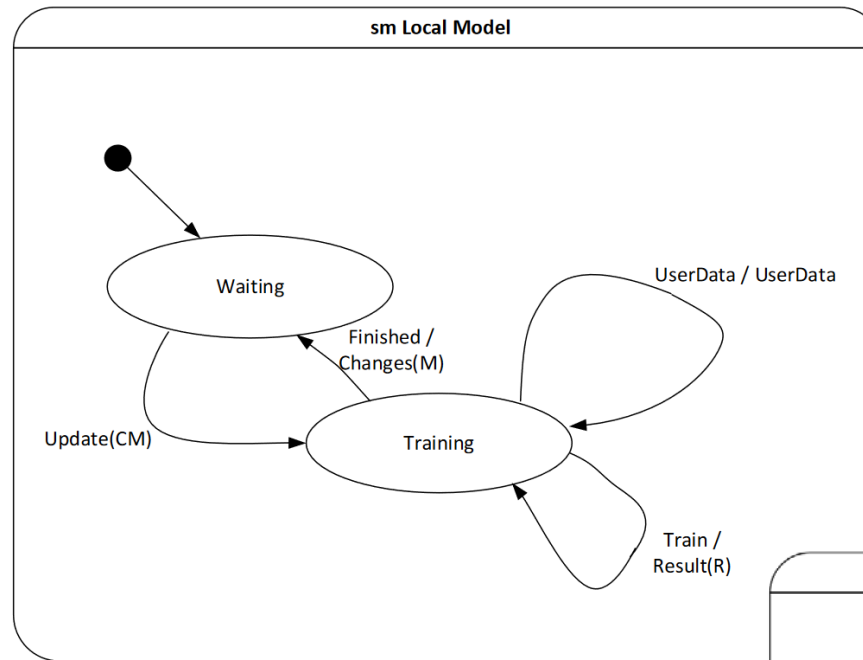


• 3c) Yes.

- The state machine may produce infinitely many traces and disallows infinitely many traces.
- Any positive trace of the lifeline may be produced. Any negative trace of the lifeline is disallowed.

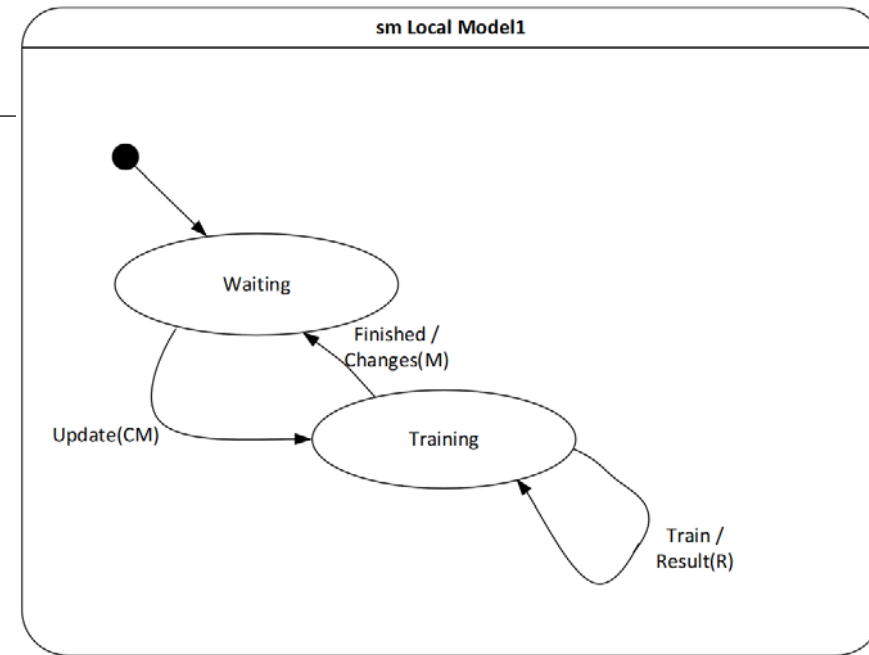


Question 4

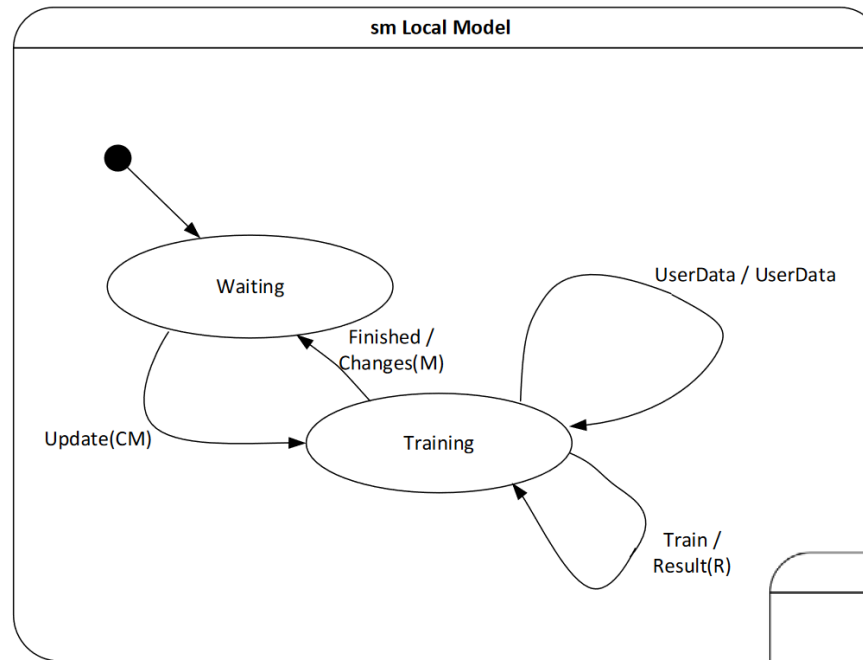


- 4a) sm Local Model1 is obtained from sm Local Model by removing one of its transitions.

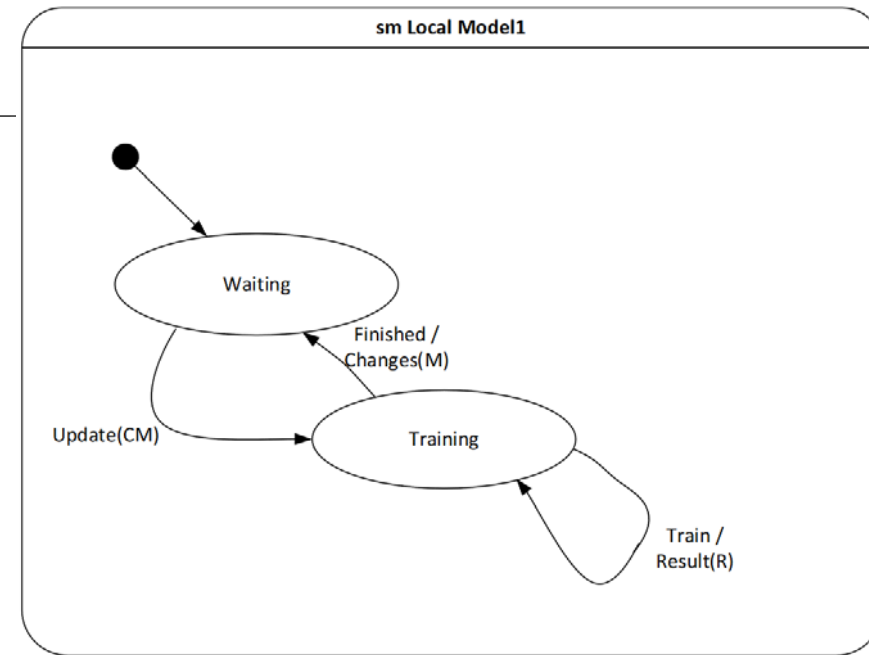
Is Local Model1 a narrowing of Local Model? Explain your answer.



Question 4



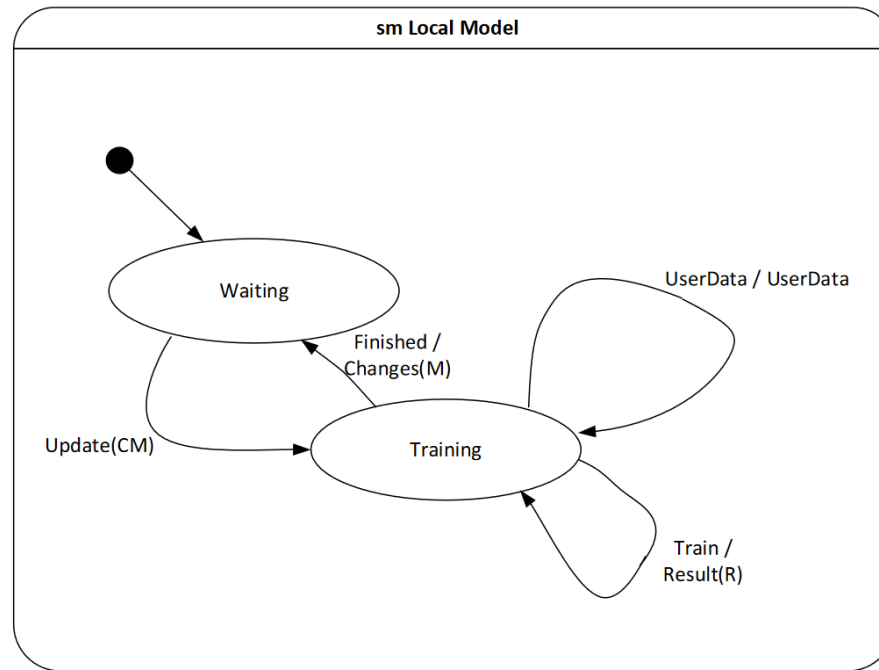
- 4a) No. The trace $\langle ?\text{Update}(\text{CM}), !\text{UserData} \rangle$ is for example positive in Local Model1 but negative in Local Model.



Question 4

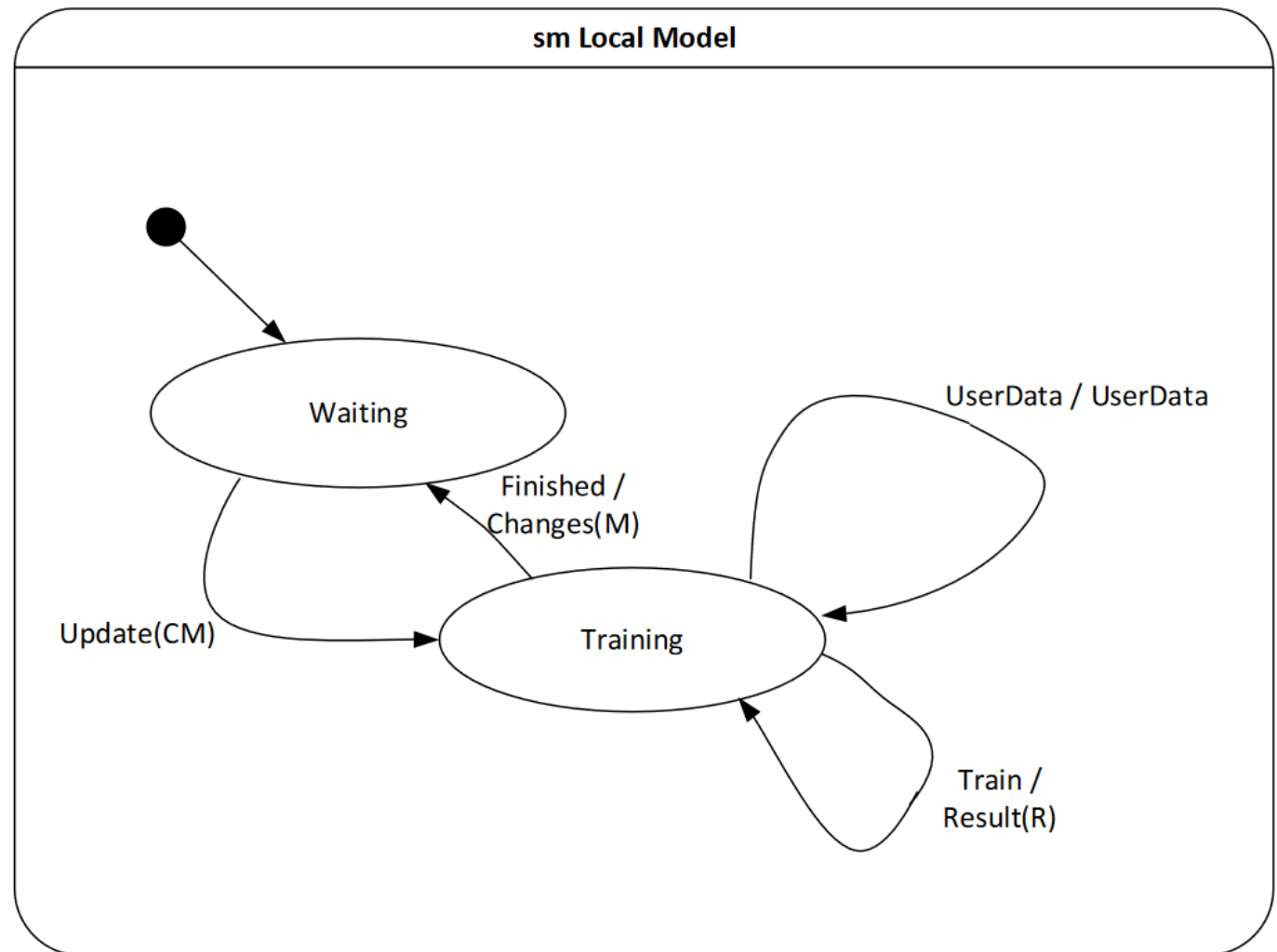
- 4b) Is it possible to draw a state machine sm Local Model2 so that Local Model2 supplements sm Local Model.

Explain your answer.

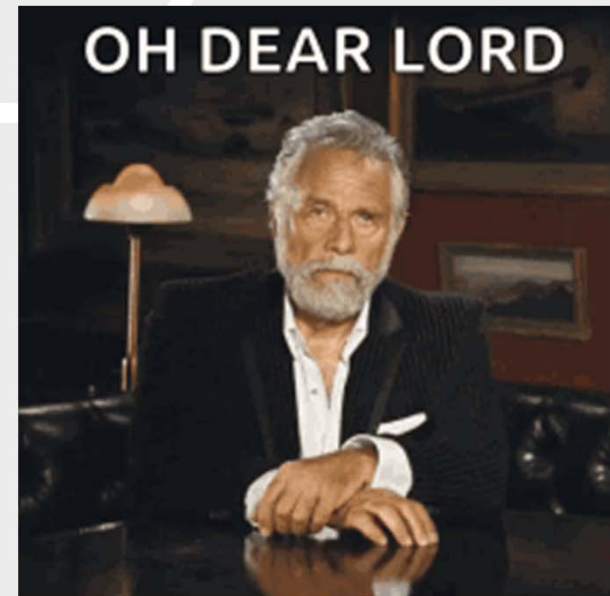


Question 4

- 4b) No. A state machine has no inconclusive traces.



Oblig III



Federated learning tldr;

- Standard AI model training
 - Collect all data on a central server -> train model -> clients/devices talk to the server to make requests, receive prediction, and sends feedback
 - Negatives of centralized setup
 - Latency, connectivity, battery, etc
- Federated learning – decentralized learning
 - User data never sent to central server
 - Model sent to clients -> client trains model using own data on its own device -> produces a new model -> sends model to server -> updates master model
 - Repeat

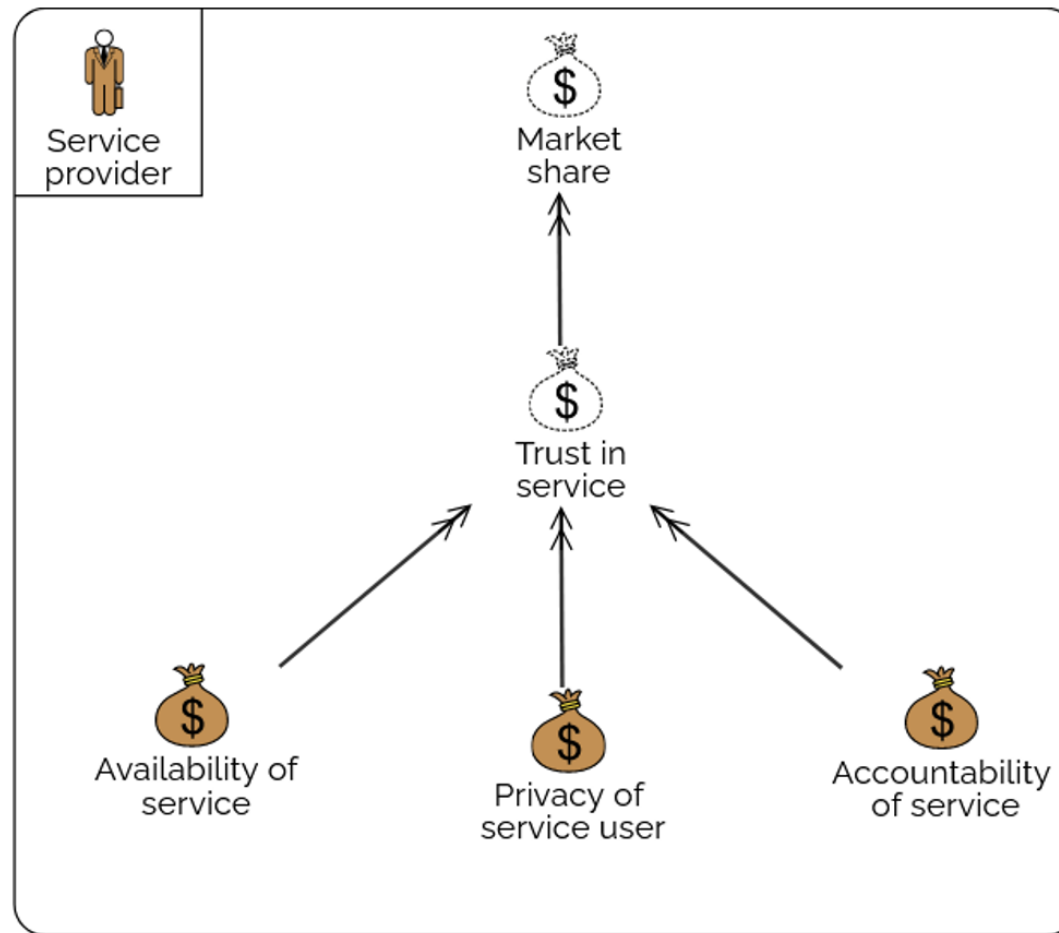
Task

- Assume you are under contract to conduct a security risk assessment of the solution for on-the-fly assistance based on federated learning that you know from Oblg-I. The risk assessment should be carried out on behalf of the service provider and should be of size 250 man-hours (for the assessors).
- Your task is to address some of these tasks as an assessor.

Question 1

- Identify at five assets of relevance for the service provider with respect to the outlined solution.
- Minimum one asset should be indirect and minimum three assets should be direct.
- Two of the direct assets should be "privacy of service user" and "accountability of service".
- One indirect asset should be "trust in service".
- Make a CORAS asset diagram that correctly relates them.

Question 1



Question 2

- Make a good qualitative scale for measuring harm (consequence) to the asset "trust in service".
- It should have at least 5 values.

Question 2

Value	Definition
Catastrophic	Scandal involving service or service provider making the headlines in national newspapers and news channels
Major	Critical coverage involving service or service provider in some major newspapers or news channels
Moderate	Critical article/coverage involving service in local or branch specific press
Minor	Considerable critical noise on social media regarding service; specific newsgroups/treads created
Insignificant	Slightly more than average noise in media

Question 3

- Make a good quantitative scale for measuring harm (consequence) to the asset "privacy of service user".
- It should have at least 5 values.

Question 3

Interval scale based on the measure: "Average fine in Euro imposed by the authorities for the incident in question"

Value	Definition of interval
Catastrophic	$<100000, \infty]$
Major	$<1000, 100000]$
Moderate	$<5, 1000]$
Minor	$<0,5]$
Insignificant	0

Question 4

- As a side-track for this question only: If your task instead is to conduct the risk assessment on behalf on the service user, to what extent should the scale from Question III be changed.

Question 4

Interval scale based on the measure: "Average percentage of private information leaked for the incident in question"

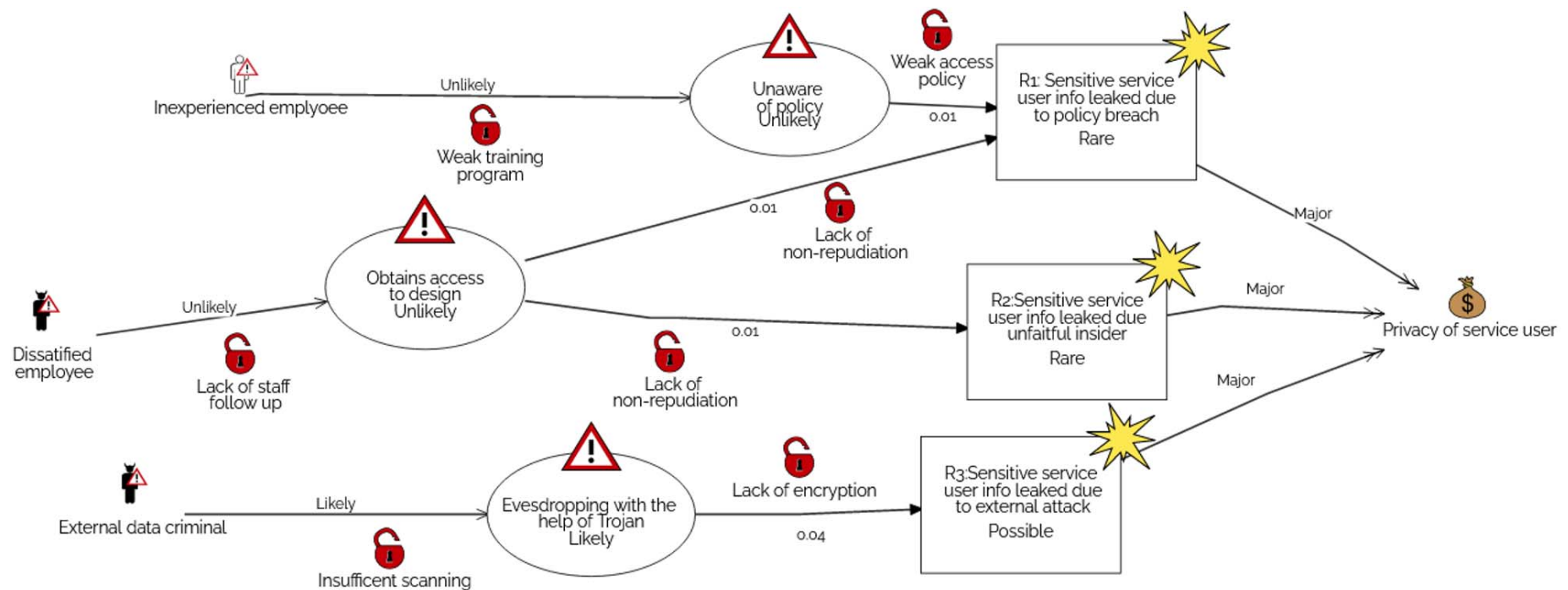
Value	Definition of interval
Catastrophic	<20,100]
Major	<10,20]
Moderate	<5,10]
Minor	<1,5]
Insignificant	[0,1]

Question 6 – reduced for time

- Make relevant threat diagrams with respect to the two direct assets "privacy of service user".
- The diagrams should all together capture at least two risks.
- The diagrams should be annotated with consequences and likelihoods in such a way that they are consistent.
- Every initiate relation, unwanted incident and threat scenario should be assigned a likelihood in the form of a frequency interval.
- Every leads-to relation should be assigned a conditional probability different from 1.
- Moreover, all initiate and leads-to relations should have at least one vulnerability associated with them (i.e. represented in the diagram).

Question 6 – reduced for time

Frequency value	Description
Common	$<12:1y, \infty:1y]$
Likely	$<1:1y, 12:1y]$
Possible	$<0.1:1y, 1:1y]$
Unlikely	$<0.01:1y, 0.1:1y]$
Rare	$[0:1y, 0.01:1y]$



Question 7

- Present the identified risks in a risk-matrix.

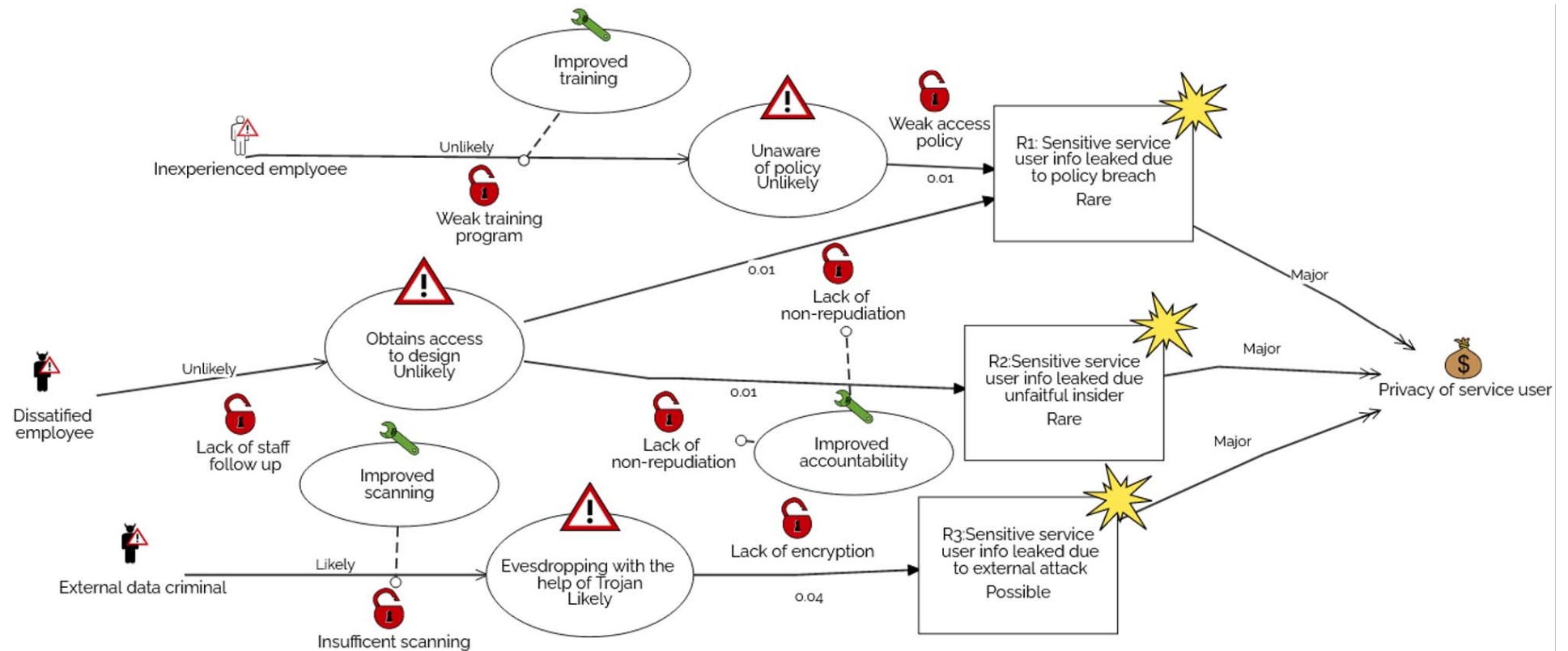
Question 7

	Rare	Unlikely	Possible	Likely	Common
Critical					
Major	R1, R2, R5		R3, R7		
Moderate					
Minor			R6	R4	
Insignificant					

Question 8

- Make a treatment diagram by annotating the threat diagrams from Question VI with relevant treatments.

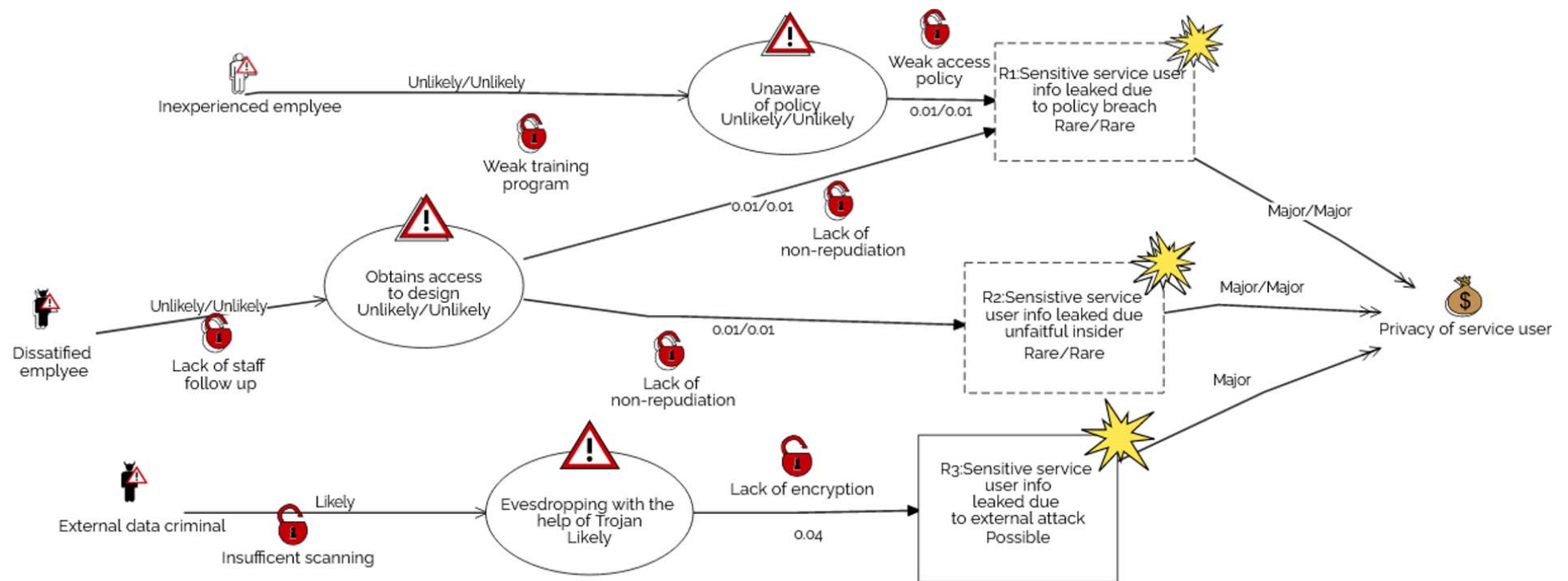
Question 8



Question 9

- Assume that the solution for on-the-fly assistance based on federated learning requires treatments for at least the most important risk.
- Use the CORAS before-after style to illustrate the effect of this treatment on the already identified risk.
- The threat diagram you have already drawn (Question VI) should correspond to the before situation.
- You are to "translate" this threat diagrams into a threat diagram expressed in the so-called before-after style reflecting the situation both before and after the implementation of the treatment.

Question 9



Questions?

- Feel free to ask questions that Ketil won't answer 😊

Good luck on oblig III!

