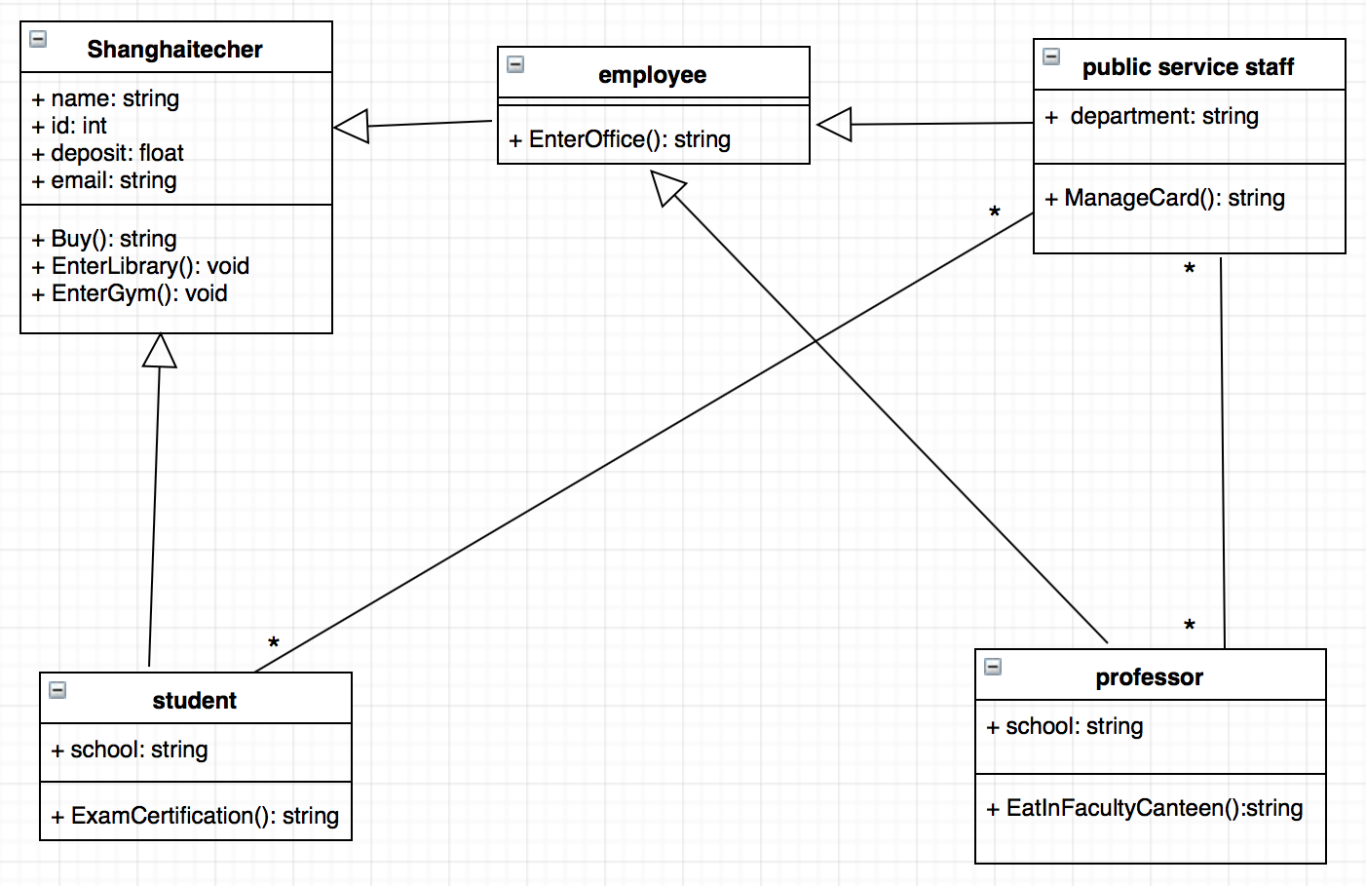
CS132: Software Engineering
HW1: UML and Risk Management

Part 1: UML Exercises (40pt)

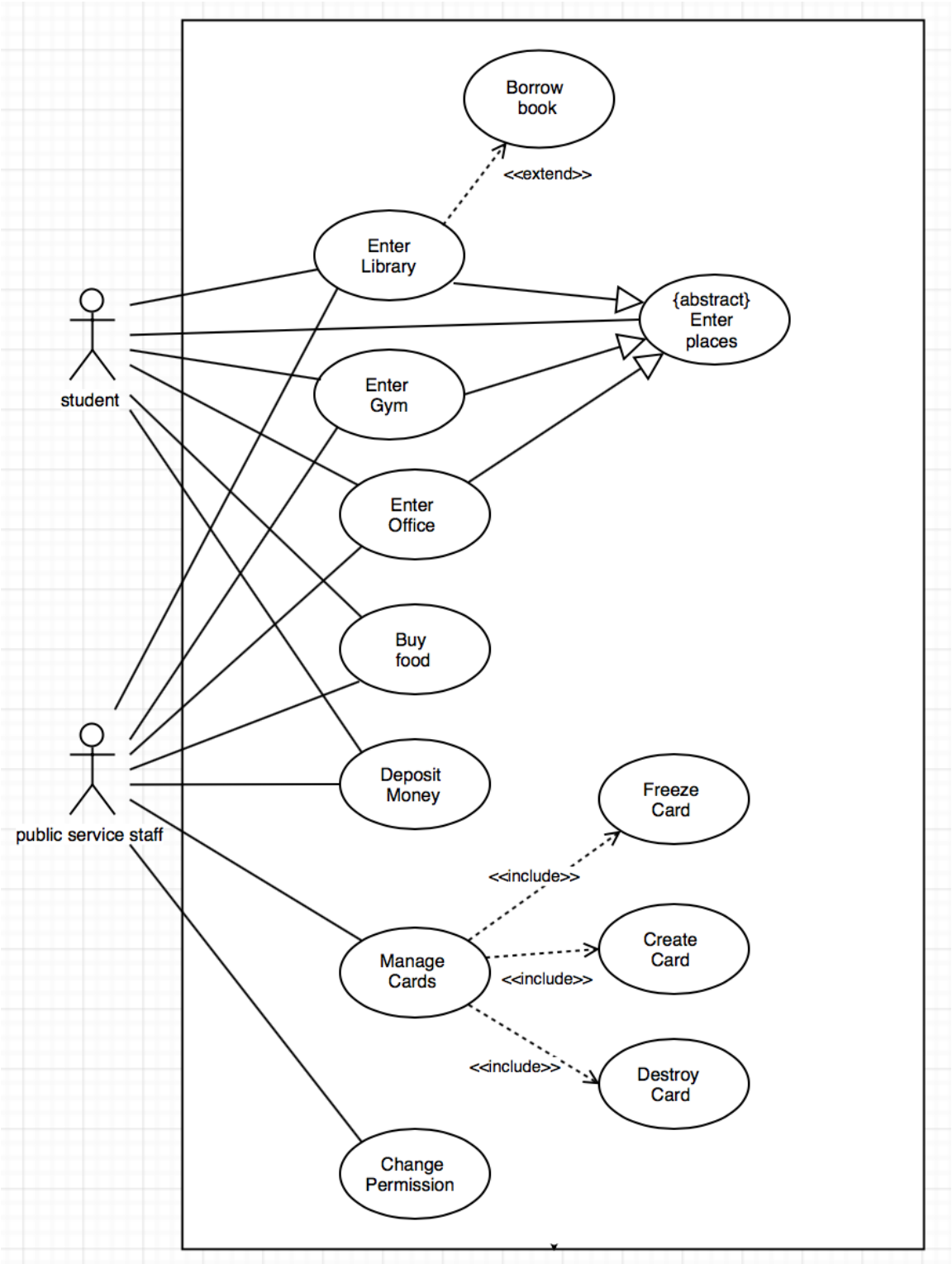
Task 1: Who is using the system and what are the relationships among them? (10pt)

Note: Your answer should not be exactly same as the reference answer.



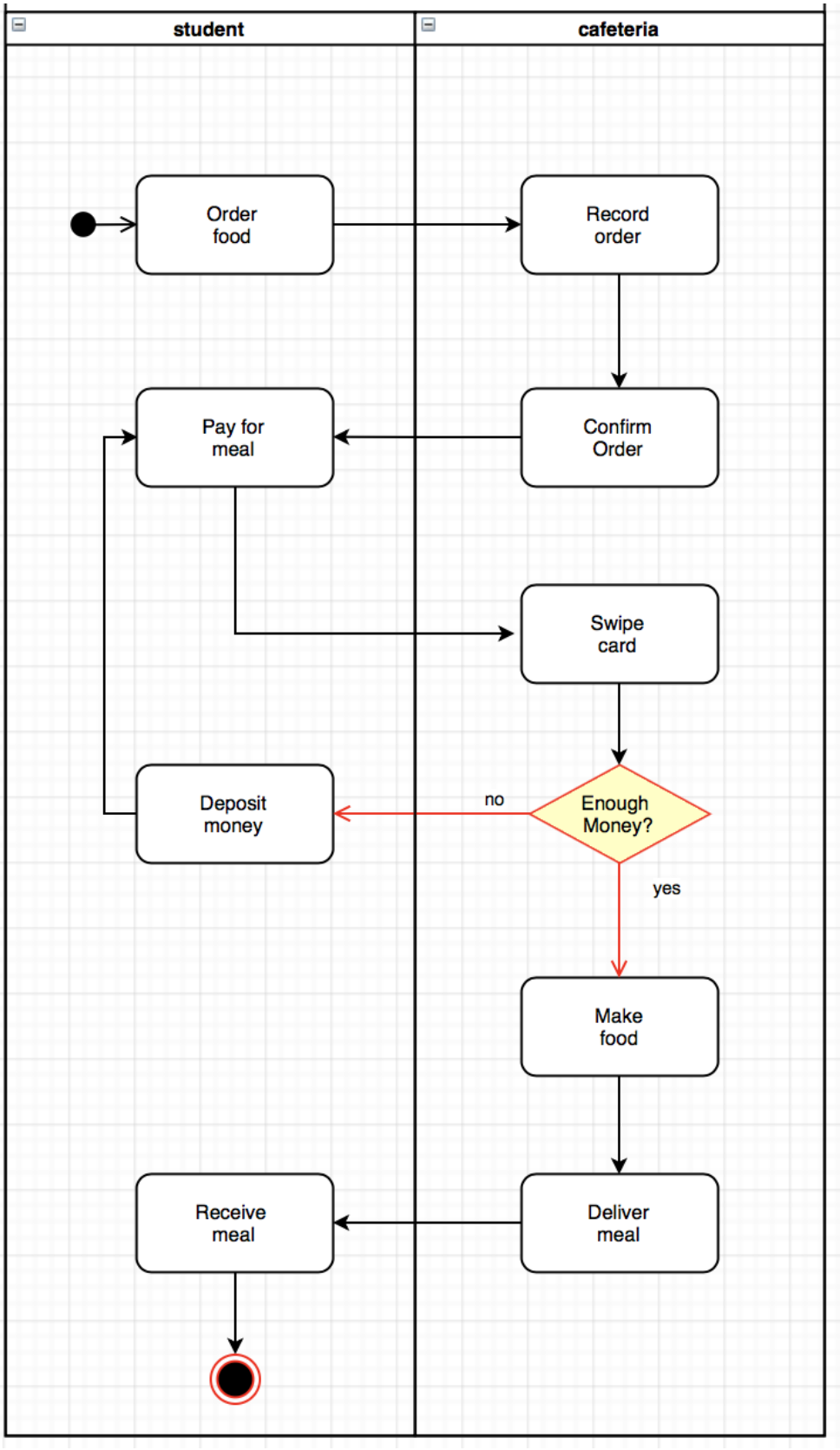
Task 2: What you can do with your campus card? (10pt)

Note: Your answer should not be exactly same as the reference answer.



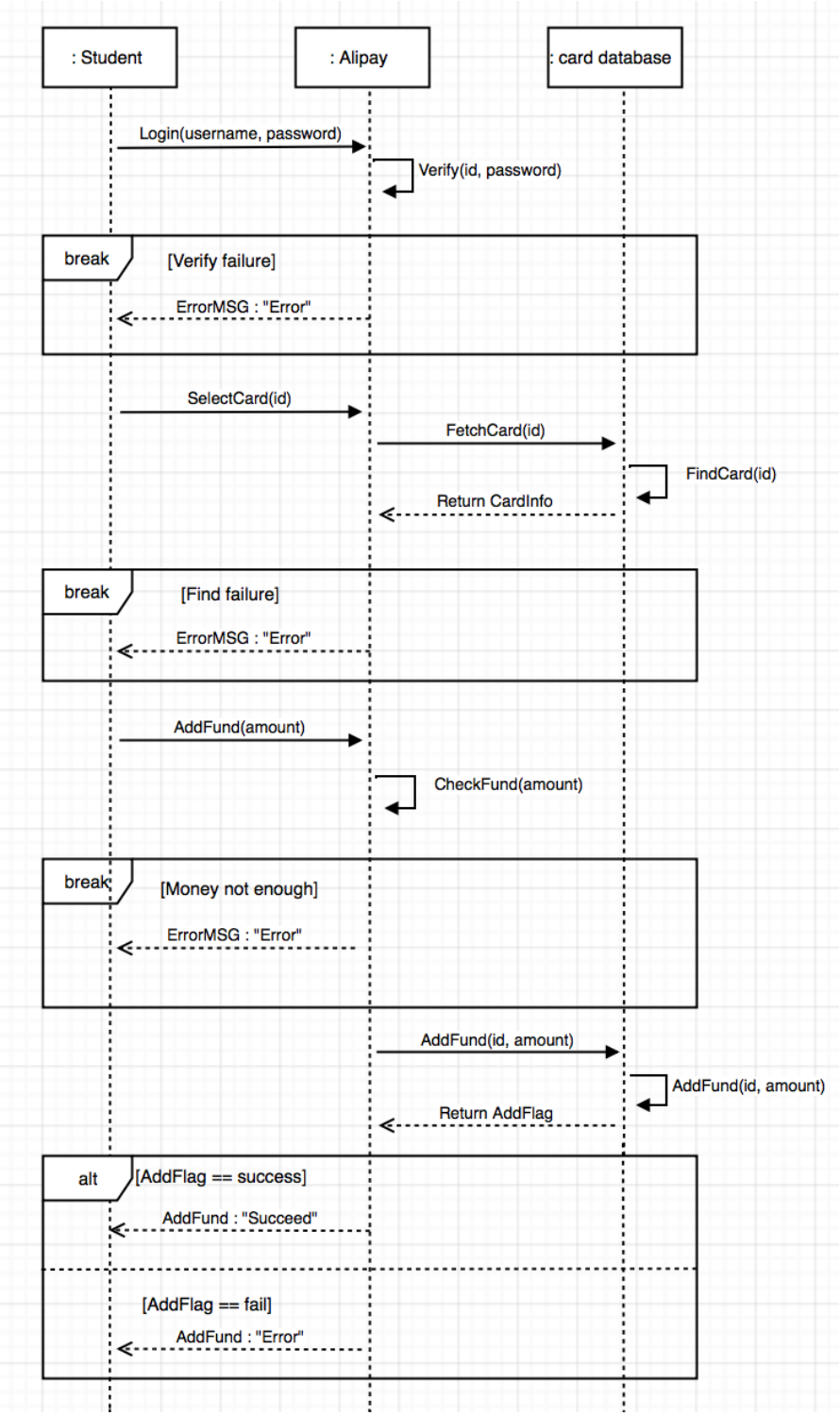
Task 3: How do you eat in the cafeteria? (10pt)

Note: Your answer should not be exactly same as the reference answer.



Task 4: How do you add fund to your campus card? (10pt)

Note: Your answer should not be exactly same as the reference answer.



Part2: Risk Management

Risk analysis:

(1) For 737-MAX:

1. **Angle of attack** exceeds the max value
2. Sensor failure or pilot negligence, this problem has not been detected
3. Excessive AOA leads to staling

For 737-800:

1. **Angle of attack** exceeds the max value
2. Sensor failure or driver negligence, this problem has not been detected
3. Excessive AOA leads to staling

They are not the same as the reason lead the first point to occur is different.

For 737-MAX, due to the adjustment of center of gravity and new engine LEAP-1B's power increasing without overall optimization, its AOA is easy to passively raise.

But for 737-800, the system design is more reasonable and the AOA will only rise in the event of an accident, such as dangerous weather, take-off and landing accidents, etc.

(2) Assume reasonable probabilities for each of the events in the sequences, calculate the risks for both 737-MAX and 737-800.

For 737-MAX, prob for 1,2,3 are 0.5, 0.1, 0.1, risk is 0.005

For 737-800, prob for 1,2,3 are 0.1, 0.1, 0.1, risk is 0.001

Risk Control Measures (RCM)

1. Preventive measures, as Reduce probability - Y; Reduce severity - N (Some students may select mitigate measures, it will be OK if the explanation is justified)
2. The first part, which makes the AOA to increase.

   Hazard: Encounter an accident

   Hazardous situation: aircraft stalling

   Sequence of events:

   1. Encounter extreme weather or serious aircraft breakdown
   2. Pilot and MCAS cannot maintain a proper AOA

3. Unable to gain motivation from air, aircraft stalling

Harm:

1. Discomfort (Minor)
2. Unstable (Major)
3. Accident (Catastrophic)

In this risk analysis, if student calculate the probability or severity, the probability of the part about the new unreasonable design(gravity or engine) shoule be decreased obviously.

Residual Risk Evaluation

New sequence for 737-MAX:

1. Sensor is not working correctly
2. MACS always making the aircraft pitchdown
3. Pilot competes with MCAS for control and constantly adjusts flight angle
4. AOA exceeds the limit during the competition

Risk analysis:

Hazard: Sensor is not working correctly

Hazardous situation: Aircraft stalling

Sequence of events:

1. Sensor is not working correctly
2. MACS always making the aircraft pitchdown
3. Pilot competes with MCAS for control and constantly adjusts flight angle
4. AOA exceeds the limit during the competition

Harm:

1. Discomfort (Minor)
2. Unstable (Major)
3. Accident (Catastrophic)

$P_{death} = P_{e1} \times P_{e2} \times P_{e3} \times P_{e4} \times P_h = 0.01 \times 0.99 \times 0.99 \times 0.5 \times 0.3 = 0.0015$

New RCM

Corrective measures

Open question: Adding other ways to ensure the reliability of MCAS, the failure of sensors needs to take into account and design other solutions to avoid the corresponding risks; provide mandatory MCAS training to ensure that pilots can close MCAS easily; avoid the use of MCAS, adjust the structure Of 737-MAX aircraft.