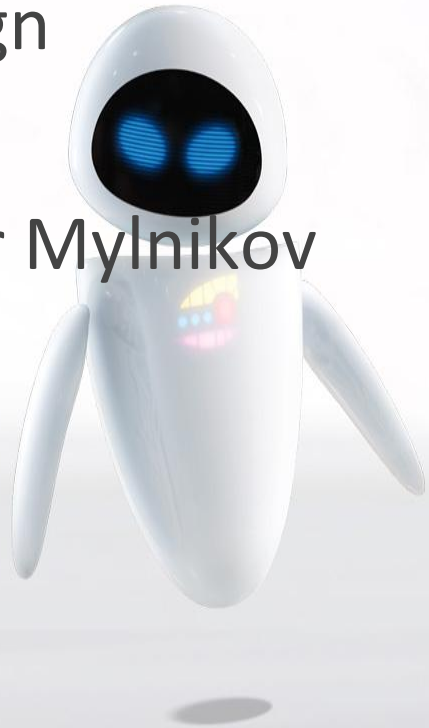
ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

The Robot

Model-Based System Design

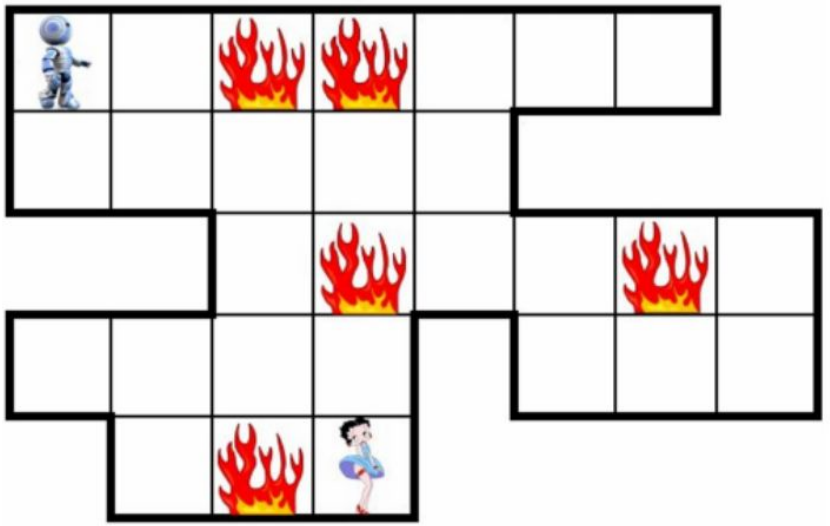
Course Project

Junxiong Wang, Wei Ma, Aleksandr Mylnikov



World Characteristics

- Environment is made of cells with temperature
- Firestorm can change it’s location
- There is the limit of temperature which causes
- There are victims of firestorm the Robot death
- Firestorm never ends



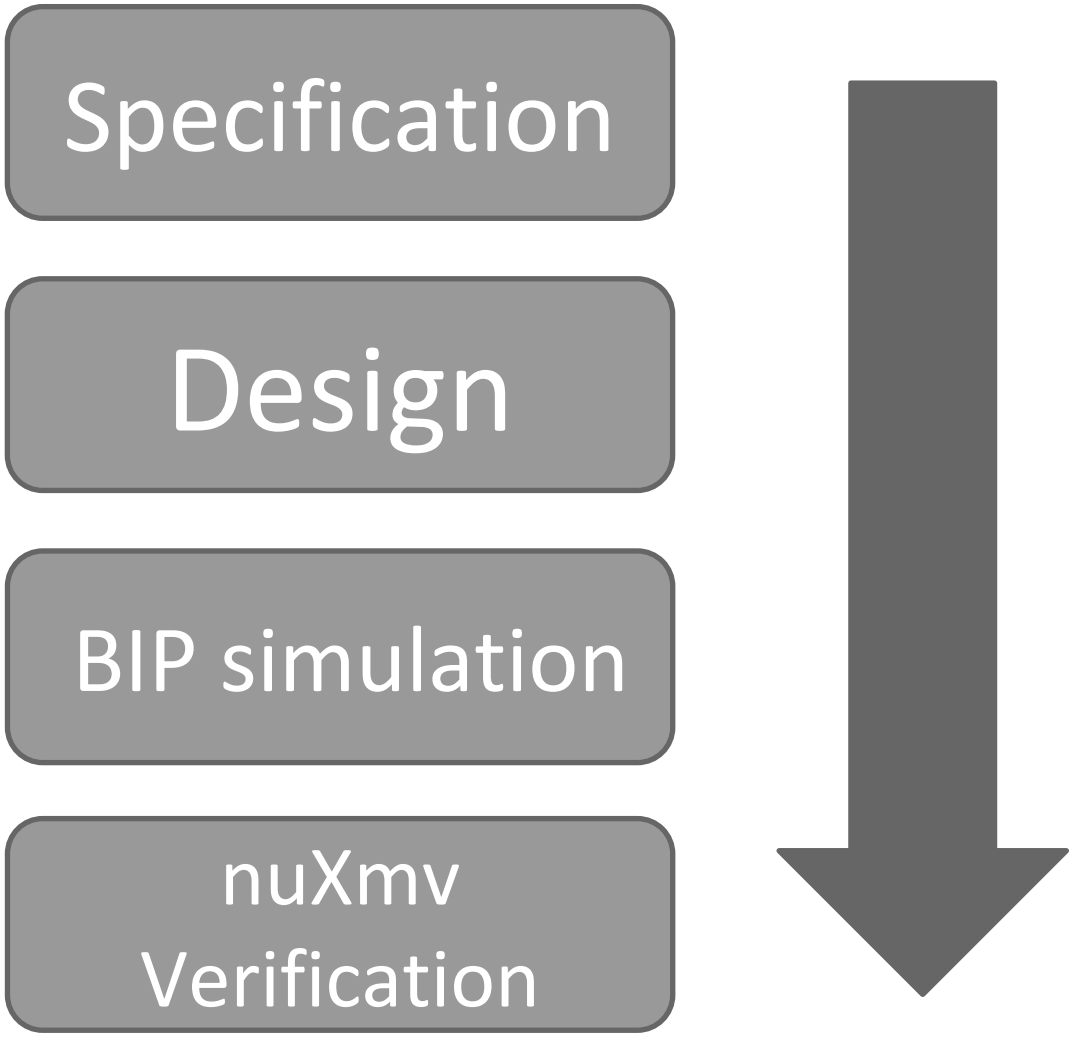
Project goals

- Practice in model system development
- Get experience in LTS design
- Get into BIP simulation
- Verify constructed model
- Let the Robot survive!

Project requirements

- Componentized model with operational semantics should be presented
- Verification and safety validation should be done
- Designed system shouldn’t have any deadlocks
- Executable code should be generated
- Additional assumptions could be made
- Designed system should be modular

Project process



The Robot

Specification

- The Robot is square with size of one cell
- The Robot has 4 sensors by each side
- All the Robot’s equipment lays inside the Robot
- The Robot could move only forward (by one side)
- The Robot could rotate one direction

Safety point list

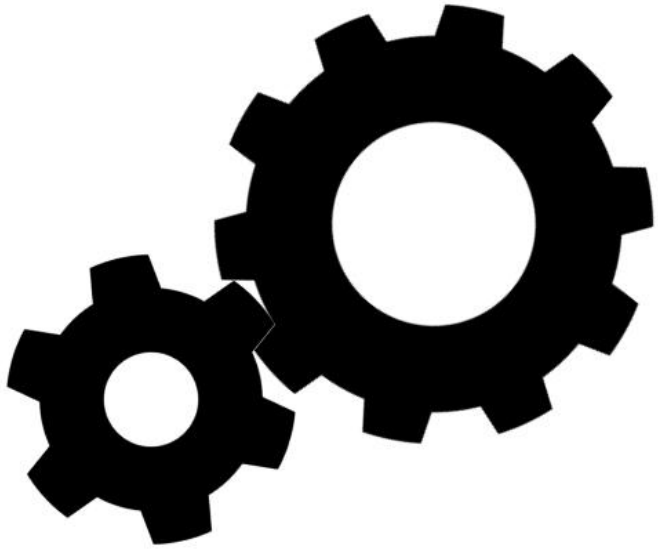
- The Robot must not advance and rotate at the same time.
- The Robot must not leave its predefined mission area.
- The Robot must not crash into walls.
- The Robot must remain in zones, where the heat intensity is below the robot’s failure level.
- When the Robot finds a victim it must transmit their location to the rescue mission control center.
- The Robot operation must always be based on recent measurement information

Assumptions

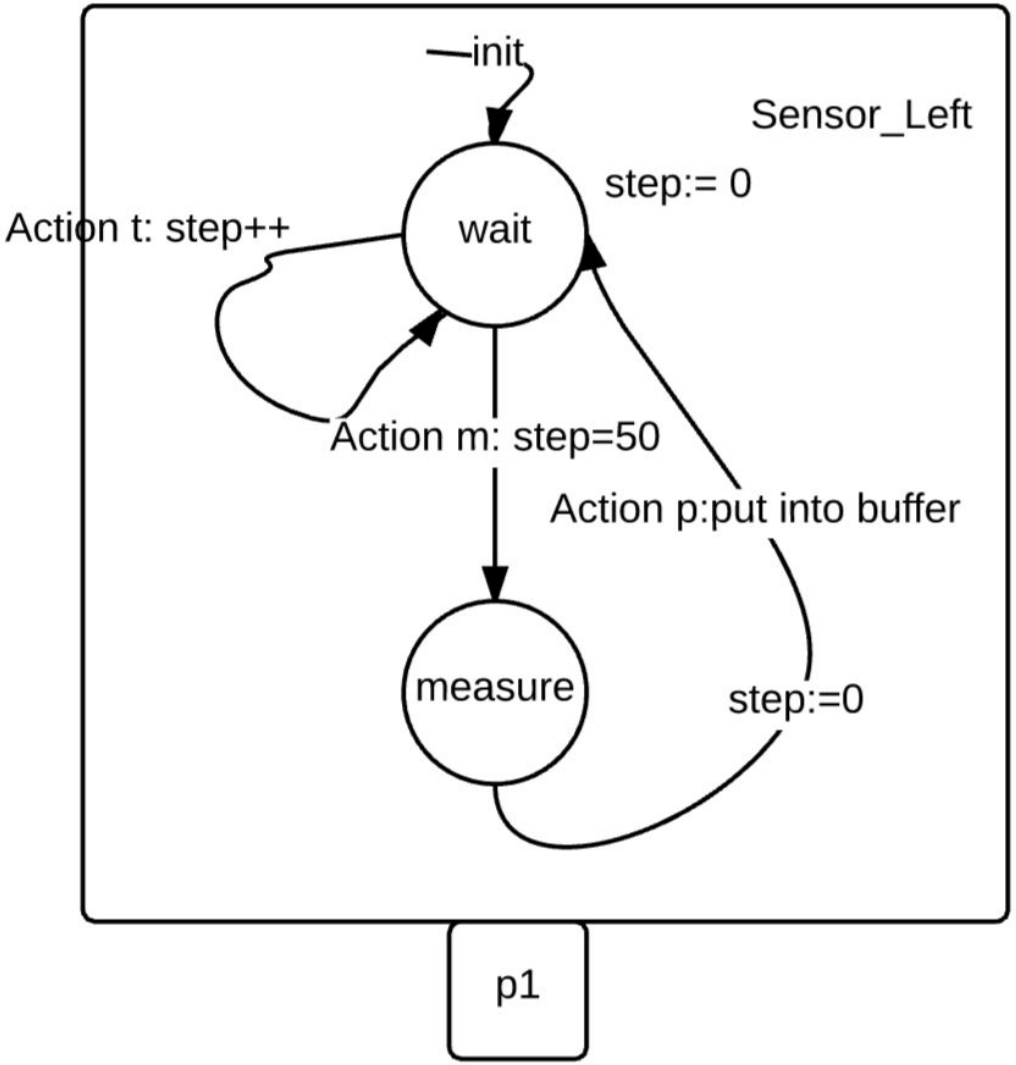
- The world has no time
- NO modules could fail, even a sensor that measures over limit temperature
- The cell of the Robot cannot become in fire
- System progress takes place once it has valid synchronization or interleaving progress possibility.

Design

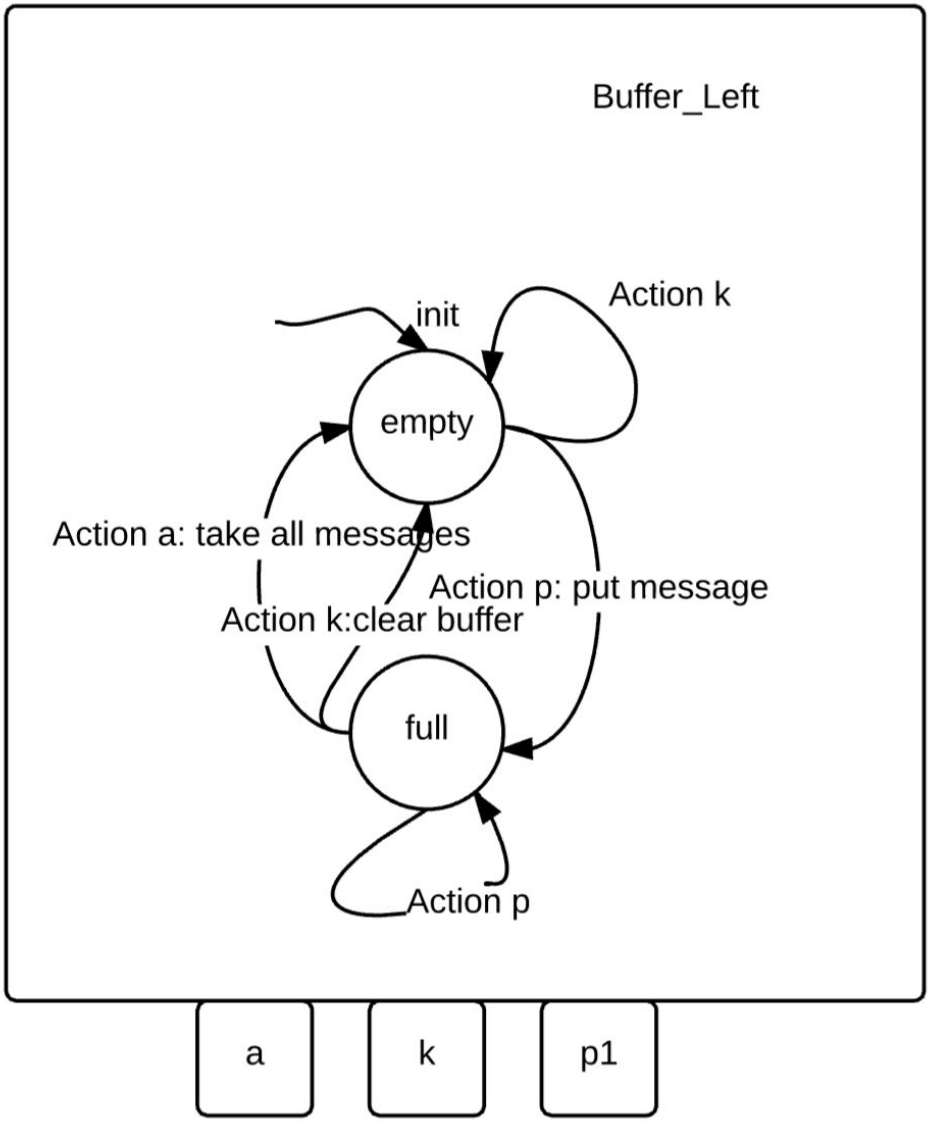
- For the Robot system we picked out following basic modules:
  - Engine
  - Navigation System
  - Search Algorithm
  - Transmitter
  - 4 Buffers
  - 4 Heat Sensors



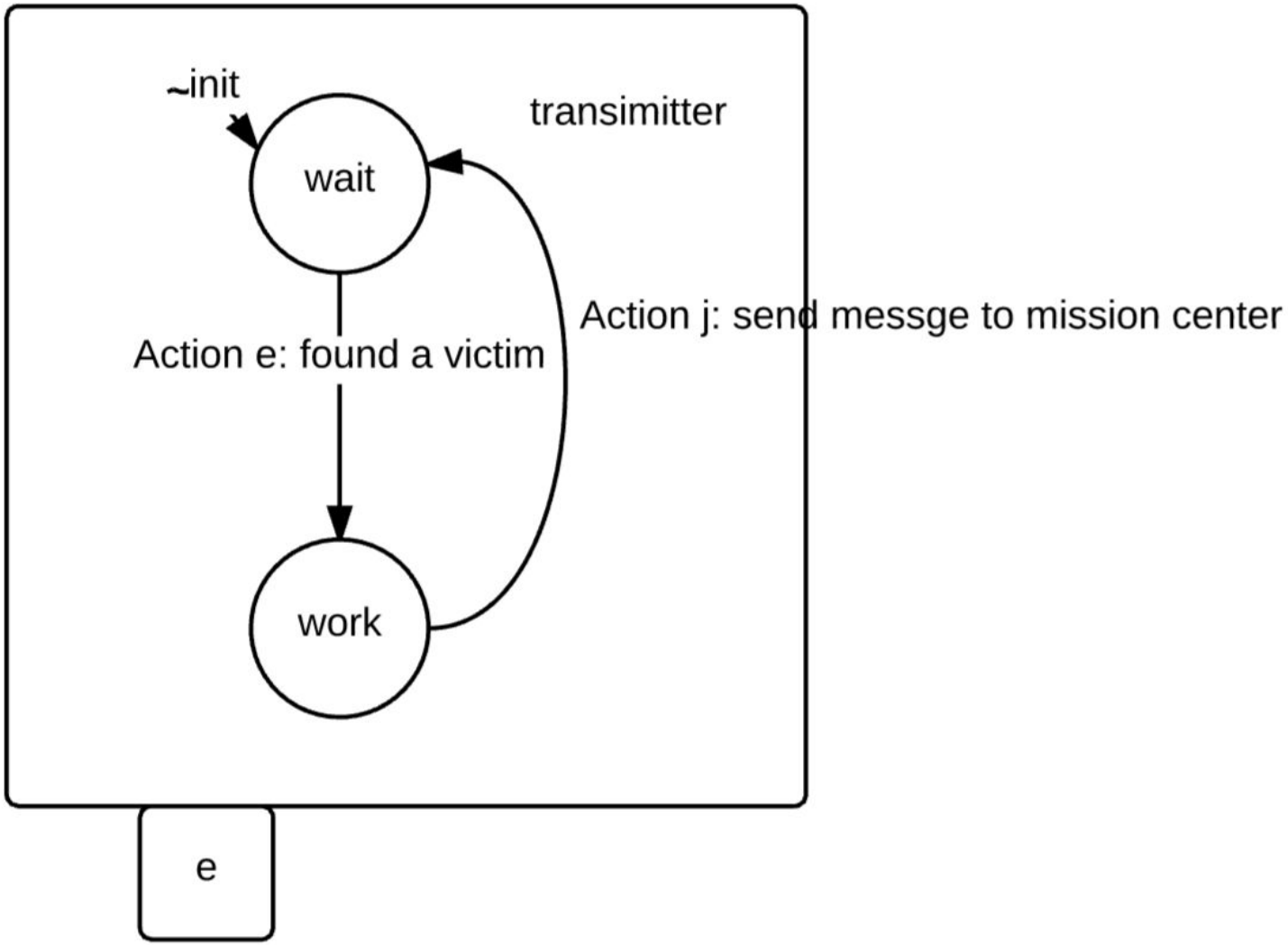
Heat Sensor


init
Sensor_Left
step:= 0
Action t: step++
wait
Action m: step=50
Action p:put into buffer
measure
step:=0
p1

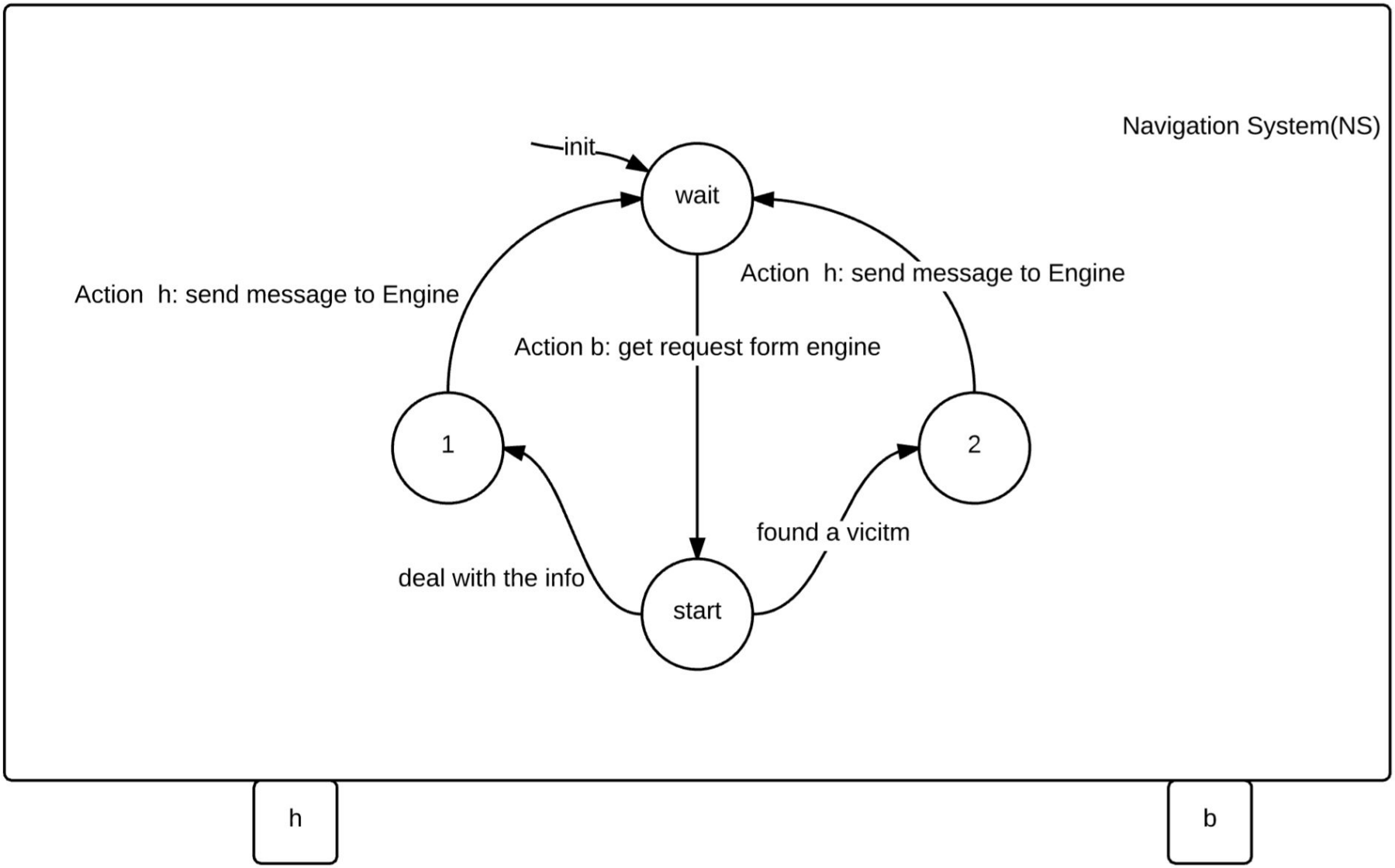
Buffer


Buffer_Left
init
Action k
empty
Action a: take all messages
Action p: put message
Action k:clear buffer
full
Action p
a
k
p1

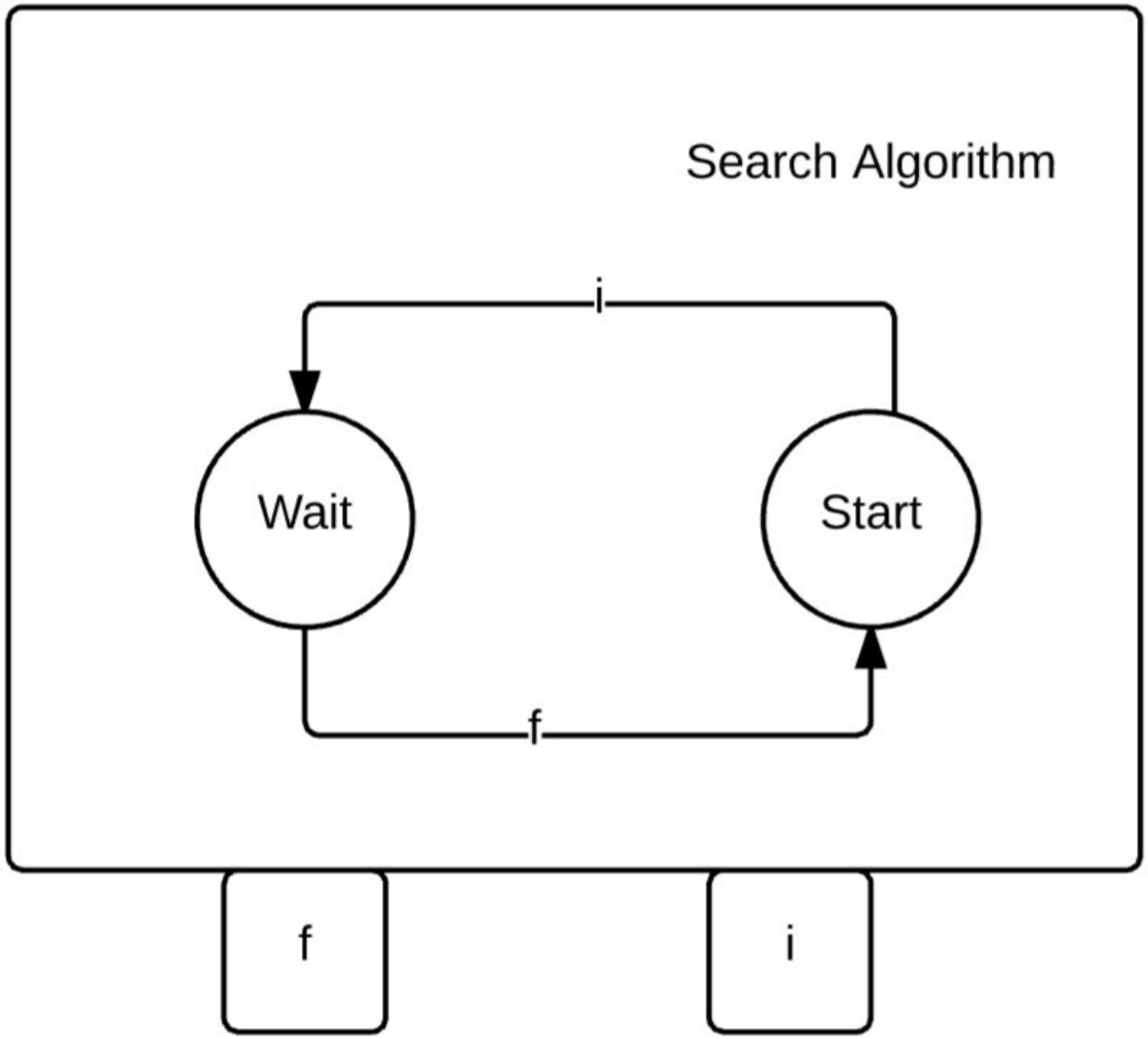
Transmitter



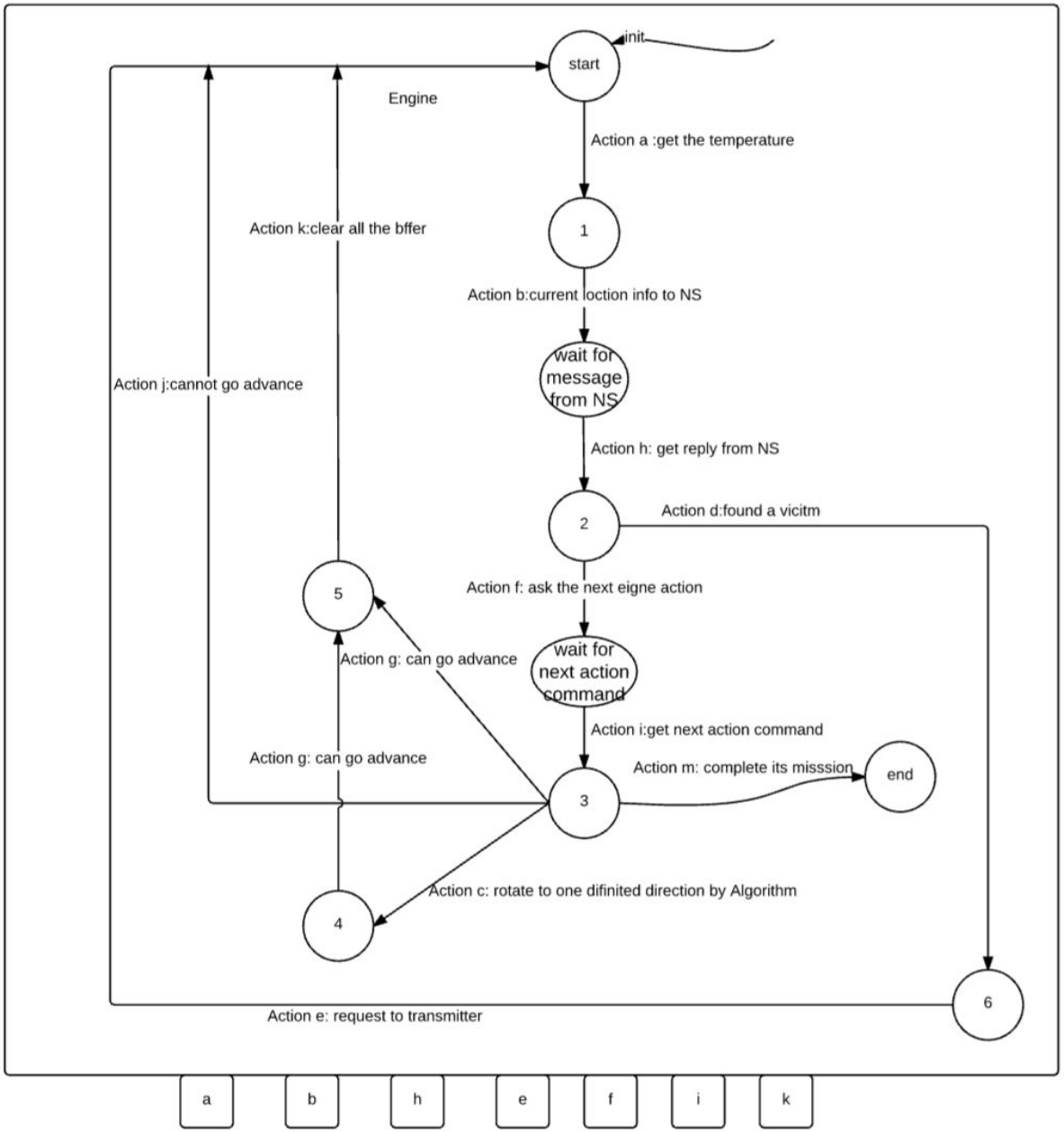
Navigation System



Search Algorithm



Engine


init
start
Engine
Action a :get the temperature
1
Action b:current loction info to NS
wait for message from NS
Action h: get reply from NS
2
Action d:found a vicitm
Action f: ask the next eigne action
wait for next action command
Action i:get next action command
3
Action m: complete its misssion
end
Action c: rotate to one difinited direction by Algorithm
4
5
Action g: can go advance
Action g: can go advance
Action k:clear all the bffer
Action j:cannot go advance
6
Action e: request to transmitter
a
b
h
e
f
i
k

Code Part

We developed BIP Simulation code which was tested to been correct for execution.

Designed model was successfully implemented with BIP language

In-between

In-between (Translation)

- Unfortunately, because of technical issues we spent huge time to correctly translate BIP simulation structure into SMV format for verification procedure.

Verification

1. Verification was made by nuXmv tool.
2. Because of NP-hard of problem verification became very time consuming operation.
3. Unfortunately, we were not able to produce one verification because of lack computational resources.

The Robot physically could die, however in case of correct Search Algorithm this state is unreachable

Verification 1

During verification stage we checked following specifications:

1. (P) System complete deadlock-freedom
2. (P) Once the robot finds a victim, it must transmit their location to the rescue mission control centre.
3. (P) Once the robot go advance, it should measure the temperature and send the command to navigation system again.

Verification 2

4. (O) No Starvation for action rotate
5. (O) The robot can't go advance if the temperature measurement over the limit
6. (O) The robot must not crash in walls

Conclusion

- We built correct modular simulation model of firefighter robot. It respects specification and requirements
- During project progress our team got practice experience in model design, BIP simulation development and SMV verification.

Question Time

Thank you for attention!