```
MACHINE
  Machine1
REFINES
  Machine0
SEES
  Context1
VARIABLES
  Flag
  Pressure
  Heater
  TimeStamp
  Delta
  NextHeater
INVARIANTS
  inv1_1   :   Flag ∈ FlagSet      //   Controls if system is in sensor or control mode, REQ 6
  inv1_2   :   (Flag = Sens ∧ Pressure ≥ 61) ⇒ (Heater = Off)      //   REQ 1 with support for modes
  inv1_3   :   (Flag = Sens ∧ Pressure ∈ {56, 57, 58, 59, 60} ∧ Heater ≠ Off) ⇒ (Heater = Low)      //   REQ 3 with support for m
  inv1_4   :   (Flag = Sens ∧ Pressure ∈ {50, 51, 52, 53, 54, 55} ∧ Heater ≠ Off) ⇒ (Heater = High)      //   REQ 2 with support
  inv1   :   Delta ∈ {−2, −1, 0, 1, 2, 3}      //   Used to change the pressure in a deterministic manner
EVENTS
  INITIALISATION   ≙
  STATUS
   ordinary
  BEGIN
   act1   :   Pressure ≔ 55
   act2   :   Heater ≔ High
   act3   :   TimeStamp ≔ 0
   act5   :   Delta ≔ 0
   act4   :   Flag ≔ Cont
   act6   :   NextHeater ≔ High
  END

  PressureSens   ≙
  STATUS
   ordinary
  REFINES
   PressureSens
  WHEN
   grd1   :   Flag = Sens      //   Flag should be in sensor mode
   grd2   :   (Heater = High) ⇒ (Delta ∈ {0, 1, 2, 3})       //   If the heather is high the pressure should increse with 0, 1, 2
   grd3   :   (Heater = Low) ⇒ (Delta ∈ {−2, −1, 0})        //   If the heather is Low the pressure should decrease with 0, 1 or
   grd4   :   (Heater = Off) ⇒ (Delta ∈ {−1, −2})      //   If the heather is Off the pressure should decrease with 1 or 2 bar
   grd5   :   Pressure + Delta ∈ ℕ      //   Used to solve prover issue
  THEN
   act1   :   Flag ≔ Cont      //   System should be set to control mode, part of REQ 4,5
   act2   :   Pressure ≔ Pressure + Delta      //   New sensor reading
   act3   :   TimeStamp :∈ ℕ
  END

  SetHeater   ≙
   extended
  STATUS
   ordinary
  REFINES
   SetHeater
  WHEN
   grd1   :   Pressure ∈ ℕ
   grd2   :   (Pressure ≥ 61) ⇒ (NextHeater = Off)      //   REQ 1
   grd3   :   (Pressure ∈ {56, 57, 58, 59, 60}) ⇒ NextHeater = Low      //   REQ 3
   grd4   :   (Pressure ∈ {50, 51, 52, 53, 54, 55}) ⇒ NextHeater = High      //   REQ 2
   grd5   :   Flag = Cont      //   System should be in control mode
  THEN
   act1   :   Heater ≔ NextHeater
   act2   :   Flag ≔ Sens      //   System should be set to sensor mode, part of REQ 4,5
  END

  SafeShutDown   ≙         //   Needed in Machine 2
  STATUS
   ordinary
  REFINES
   SafeShutDown
  WHEN
   grd1   :   Flag = Cont
  THEN
```

```
   act1   :   Flag ≔ Sens
   act2   :   Heater ≔ Off
  END

END
```