REQUIREMENTS DOCUMENT Lab 2

Group 12

Assumptions:

- Only maximum pressure as invariant, lower pressure is allowed (only maximum pressure is critical for safety)
- Events keep the pressure in a preferred interval

inv1	Pressure <= 65
inv2	¬(pressure > 60 ∧ (nextState = TimerState ∨ nextState = SensorState)) ∨ heater = off ∨ Mode=SUPERVISED
inv3	¬(pressure > 50 ∧ pressure ≤ 55 ∧ (nextState = TimerState ∨ nextState = SensorState)) ∨ heater = high ∨ Mode=SUPERVISED
inv4	¬(pressure > 55 ∧ pressure ≤ 60 ∧ (nextState = TimerState ∨ nextState = SensorState)) ∨ heater = low ∨ Mode=SUPERVISED
inv5	¬(conTimeStamp < senTimeStamp ∧ nextState = SensorState) ∨ boilerOn = FALSE
inv6	∀x·(x ∈ ValidAddresses ⇔ x ≤ MaxAddress)

Variables: types in rodin as invariants

V10	Pressure [natural]
V15	senTimeStamp [natural]
V20	conTimeStamp [natural]
V30	boilerOn [bool]
V40	heater {high, low, off}
V50	nextState {ControllerState, SensorState, TimeState}
V60	Users ⊆ USERSET
V70	USERSET ≠ ∅
V80	ValidAddresses ⊆ Addresses
V90	MaxAddress ∈ ValidAddresses
V100	Roles = {Supervisor, Operator}

V110	Modes = {AUTOMATIC, SUPERVISED, MONITORED}
V120	Mode ∈ Modes
V130	Permissions ∈ Users → Roles

Events: set the heater state according to the current temperature

controlOff	P > 60 and nextState = ControllerState and Mode≠SUPERVISED and address is valid => h := off; increase TimeStamp; nextState = TimeStater
ControlHigh	P > 50 && P <= 55 nextState = ControllerState and and address is valid=> h := high; increase TimeStamp; nextState = TimeStater
ControlLow	P > 55 && P <= 60 nextState = ControllerState and Mode≠SUPERVISED and address is valid => h := low;; increase TimeStamp; nextState = TimeStater
SensorOff	Increase timestamp and change pressure accordingly, set package values
SensorLow	Increase timestamp and change pressure accordingly, set package values
SensorHigh	Increase timestamp and change pressure accordingly, set package values
controlTHigher	Synchronize controller local timestamp
sensorTHigher	Synchronize sensor local timestamp
Shutdown	Set boilerOn:=FALSE in case of invalid incoming timestamp of package
ManualShutdown	Allows setting of boilerOn being set to FALSE if Mode=SUPERVISED or MODE=MONITORED
Chernobyl	Sets heater to a random state if MODE=SUPERVISED
AddUser	Add newUser ∈ USERSET with newRole ∈ Roles to Users respectively newUser ↦ newRole to Permissions if newUser is not yet added to Users
switchMode Supervisor	If user has supervisor permissions, change Mode to newMode with newMode ≠ Mode
switchMode Operator	If user has operator permissions, change Mode to newMode with newMode ≠ Mode and Mode ≠ SUPERVISED