Group 17 - Software Safety and Security

Assignment 1B

https://github.com/Simoid/DD2460-Event-B/tree/assignment1b

Requirements OBJ 2 - Correspond to Machine 0/1

- REQ1 : If the pressure exceeds 61 bar, the controller has to shut down the system
- REQ2 : If the pressure is between 50 and 55, the controller has to set the heater to high
- REQ3 : If the pressure is between 56 and 60, the controller has to set the heater to low
- REQ4 : The system will be in an infinite loop that switches between the Controller and the Sensor
- REQ5 : The system should be either in the sensor or controller mode
- REQ6 : The sensor sends the pressure to the controller

Requirements OBJ 3 - Correspond to Machine 2

- REQ7 : The sensor should have a local clock.
- REQ8 : The controller should have a local clock.
- REQ9 : The sensor should generate a timestamp when sending a packet to the controller.
- REQ10 : The sensor should specify its address when sending a packet to the controller.
- REQ11 : The system will have a list of legitimate addresses that are allowed to send packets
- REQ12 : The controller should turn off the heater if the timestamp is outdated.
- REQ13 : The controller should turn off the heater if the packet comes from an address that is a part of the legitimate address list.

Requirements OBJ 4 - Correspond to Machine 3

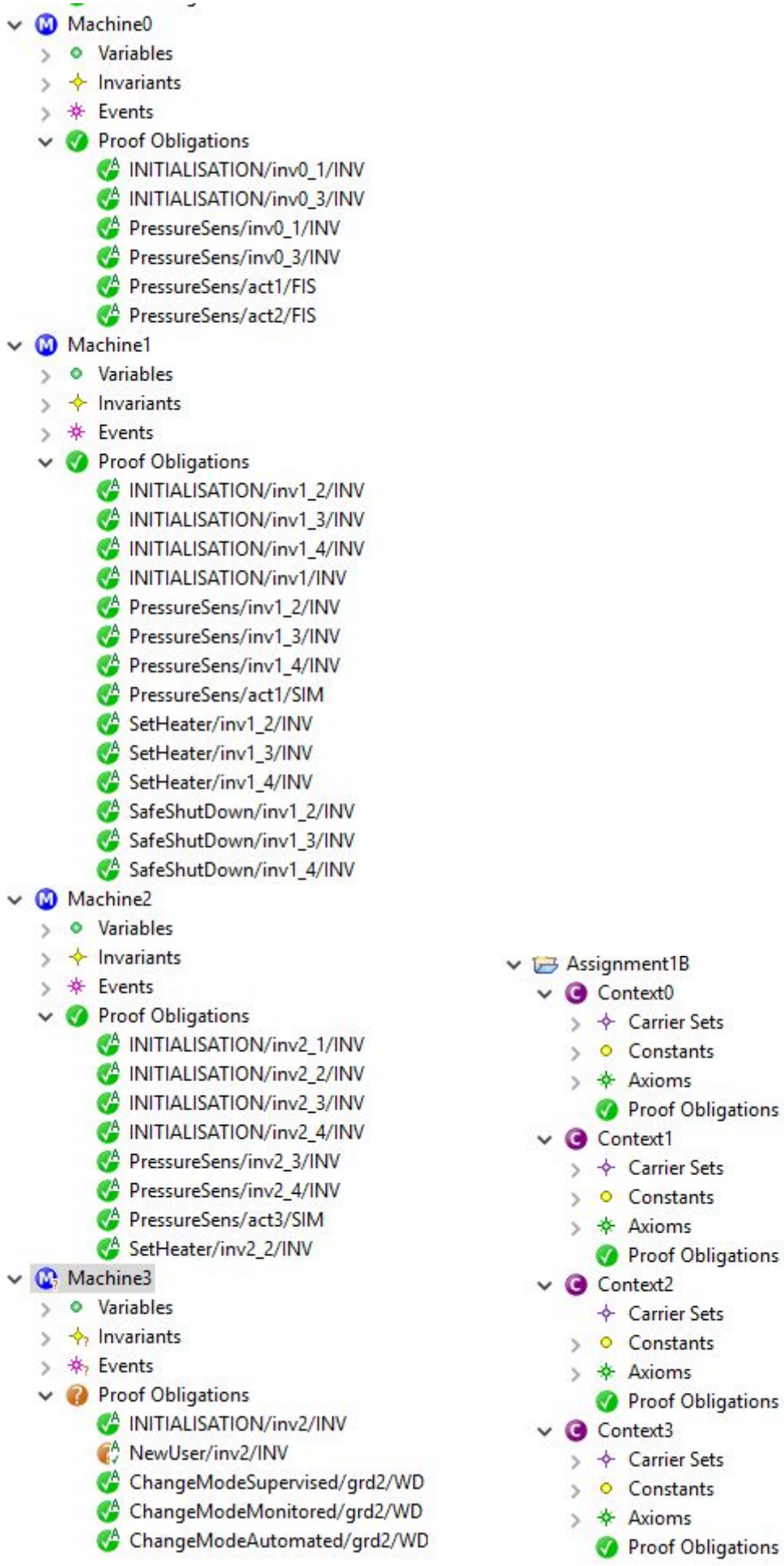
- REQ14 : The system will have users with unique identifier and different roles
- REQ15 : The system can add new users and assign them a new role
- REQ16 : An user with the role “operator” or “supervisor” can change the mode from AUTOMATED to MONITORED and vice versa.
- REQ17 : While the system is in MONITORED mode the an user with the roles “operator” or “supervisor” can switch off the heater.
- REQ18 : An user with the role “supervisor” can switch mode from AUTOMATED to MONITORED or SUPERVISED and/or back to AUTOMATED

- REQ19 : The boiler can run in three different modes, AUTOMATED, MONITORED, SUPERVISED.
- REQ20 : AUTOMATED mode will run the boiler as the previous requirements have defined

We completed Objective 1,2 and 3. We implemented half of Objective 4 : Users management and Heater Mode monitoring. We did not implement the Heater Set Events in the SUPERVISED and the CONTROLLED mode.

All of the code has been attached as PDF:s in the assignment.
The variables and events have comments that explain them.

We have one proof obligation that does not succeed (invariant 2 in machine 3). We followed the syntax and structure exactly like in Lecture 5, so we do have no understanding of why it fails. Please tell us if you figure it out.


Machine0
Variables
Invariants
Events
Proof Obligations
INITIALISATION/inv0_1/INV
INITIALISATION/inv0_3/INV
PressureSens/inv0_1/INV
PressureSens/inv0_3/INV
PressureSens/act1/FIS
PressureSens/act2/FIS
Machine1
Variables
Invariants
Events
Proof Obligations
INITIALISATION/inv1_2/INV
INITIALISATION/inv1_3/INV
INITIALISATION/inv1_4/INV
INITIALISATION/inv1/INV
PressureSens/inv1_2/INV
PressureSens/inv1_3/INV
PressureSens/inv1_4/INV
PressureSens/act1/SIM
SetHeater/inv1_2/INV
SetHeater/inv1_3/INV
SetHeater/inv1_4/INV
SafeShutDown/inv1_2/INV
SafeShutDown/inv1_3/INV
SafeShutDown/inv1_4/INV
Machine2
Variables
Invariants
Events
Proof Obligations
INITIALISATION/inv2_1/INV
INITIALISATION/inv2_2/INV
INITIALISATION/inv2_3/INV
INITIALISATION/inv2_4/INV
PressureSens/inv2_3/INV
PressureSens/inv2_4/INV
PressureSens/act3/SIM
SetHeater/inv2_2/INV
Machine3
Variables
Invariants
Events
Proof Obligations
INITIALISATION/inv2/INV
NewUser/inv2/INV
ChangeModeSupervised/grd2/WD
ChangeModeMonitored/grd2/WD
ChangeModeAutomated/grd2/WD
Assignment1B
Context0
Carrier Sets
Constants
Axioms
Proof Obligations
Context1
Carrier Sets
Constants
Axioms
Proof Obligations
Context2
Carrier Sets
Constants
Axioms
Proof Obligations
Context3
Carrier Sets
Constants
Axioms
Proof Obligations