MACHINE

VARIABLES

phase, operation, prm, stop, R_real, R_est, F_real, F_est

INVARIANTS

inv7: $(phase = checking \land prm = TRUE) \Rightarrow R\_est \leq R\_real$

EVENTS

Event Move $\langle\rangle \triangleq$

any

m

where

grd1: $phase = move$

then

act1: $phase := report$
act2: $R\_real := R\_real + m$
act3: $F\_real := F\_real + m$

end

Event Report $\langle\rangle \triangleq$

when

grd1: $phase = report$

then

act1: $phase := integrity$

end

Event Integrity $\langle\rangle \triangleq$

where

grd5: $phase = integrity$

then

act1: $phase :\in \{detection, res\}$

end

Event Res $\langle$ordinary$\rangle \triangleq$

when

grd1: $phase = res$

then

act1: $phase :\in \{detection, est\}$

end

Event Est $\langle$ordinary$\rangle \triangleq$

where

grd1: $phase = est$
grd4: $prm = TRUE \Rightarrow r\_est \leq R\_real$

then

act1: $phase := checking$
act2: $R\_est := r\_est$

end

Event Detection $\langle$ordinary$\rangle \triangleq$

when

grd1: $phase = detection$

then

act1: $phase := move$
act2: $operation := abnormal$

end

Event Checking $\langle$ordinary$\rangle \triangleq$

where

grd1: $phase = checking$
grd3: $R\_est > R\_real \Leftrightarrow s = TRUE$

then

act1: $phase := move$
act2: $stop := s$

end

END

2