Alex Dussault, 26671985

Jonathan Hamel, 26627900

Assignment 3 Specifications

Safety\_Critical\_Room

S = (*Q, Σ1*, *Σ2* , q0 , *V , Λ* ),

where

*Q*  = {dormant, init, idle, monitoring, error\_diagnosis, safe\_shutdown}

*Σ1* = { start, init\_ok, init\_crash, begin\_monitoring, idle\_crash, monitor\_crash, idle\_rescue, moni\_rescue, retry\_init, shutdown, sleep, kill }

*Σ2*  = { retry :=0, init\_err\_msg, idle\_err\_msg, moni\_err\_msg, retry++ }

*V* = { *retry*: N0, inlockdown: Boolean}

*Λ*: Transition Specifications

1. idle error\_diagnosis
2. monitoring error\_diagnosis
3. error\_diagnosis idle
4. error\_diagnosis monitoring
5. error\_diagnosis init
6. error\_diagnosis safe\_shutdown
7. safe\_shutdown dormant
8. dormant exit
9. monitoring exit

Refined init

S = (*Q, Σ1*, *Σ2* , q0 , *V , Λ* ),

where

*Q*  = {boot\_hw, senchk, tchk, psichk, ready}

*Σ1* = { hw\_ok, sen\_ok, t\_ok, psi\_ok}

*Σ2*  = { }

*V* = { *hardware modules = {ok, not ok}, sensors = {ok, not ok}, temperature sensors = {ok, not ok}, pressure sensors = {ok, not ok}*}

*Λ*: Transition Specifications

1. boot\_hw senchk
2. senchk tchk
3. tchk psichk
4. psichk ready
5. ready exit

Refined monitor

S = (*Q, Σ1*, *Σ2* , q0 , *V , Λ* ),

where

*Q*  = {monidle, regulate\_environment, lockdown }

*Σ1* = {after(1000ms), no\_contagion, contagion\_alert, after(100ms), purge\_succ}

*Σ2*  = { FACILITY\_ERR\_MSG, inLockdown = true, inLockdown = false}

*V* = {inLockdown: Boolean, hasContagion: Boolean}

*Λ*: Transition Specifications

1. monidle regulate\_environment
2. monidle lockdown
3. regulate\_environment monidle
4. lockdown lockdown
5. lockdown monidle

Refined lockdown

S = (*Q, Σ1*, *Σ2* , q0 , *V , Λ* ),

where

*Q*  = {prep\_vpurge, alt\_psi, alt\_temp, risk\_assess, safe\_status }

*Σ1* = {initiate\_purge, psicyc\_comp, tcyc\_comp }

*Σ2*  = {lock\_doors, unlock\_doors}

*V* : risk: ℝ.

*Λ*: Transition Specifications

1. prep\_vpurge
2. prep\_vpurge alt\_psi
3. prep\_vpurge alt\_temp
4. alt\_psi risk\_assess
5. alt\_temp risk\_assess
6. risk\_assess prep\_vpurge
7. risk\_assess safe\_status
8. safe\_status exit

Refined error diagnosis

S = (*Q, Σ1*, *Σ2* , q0 , *V , Λ* ),

where

*Q*  = {error\_rcv, reset\_module\_date, applicable\_rescue }

*Σ1* = {reset\_to\_stable, apply\_protocol\_rescue }

*Σ2*  : reset kernel module data.

*V* : err\_protocol\_def: Boolean.

*Λ*: Transition Specifications

1. error\_rcv
2. error\_rcv reset\_module\_data
3. error\_rcv applicable\_rescue
4. reset\_module\_date exit
5. applicable\_rescue exit