Thomas Chapados

Leo Yu

Assignment 3 Specification

Safety Critical Room

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

q0: dormant

∑1: {start, init\_ok, init\_error, retry\_init, idle\_crash, idle\_rescue, begin\_monitoring, monitor\_crash, monitor\_rescue, kill, idle\_err\_msg, monitor\_err\_msg }

∑2: {shutdown, retry++}

V: retry: N0;

Ʌ: Transition specifications

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

Refined init

Q: {boot\_hw, senchk, tchk, psichk, ready}

q0: boot\_hw

∑1: {hw\_ok, senok, t\_ok, psi\_ok}

Ʌ: Transition specifications

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

refined monitor

Q: {monidle, regulate\_enviroment, lockdown}

q0: monidle

∑1: {after, no\_contagion, contagion\_aler, purge\_succ}

∑2: {FACILITY\_CRIT\_MESG}

V: islockdown: boolean;

Ʌ: Transition specifications

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

Error diagnosis

Q: {error\_rcv, applicable\_rescue, reset\_module\_data}

q0: errpr\_rcv

∑1: {apply\_protocol\_rescues, rest\_to\_stable}

V: err\_protocol\_def: boolean;

Ʌ: Transition specifications

1. error\_rcv
2. error\_rcv applicable\_rescues
3. error\_rcv reset\_module\_data

Lockdown

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

q0: prep\_vpurge

∑1: {initia\_purge, tcyc\_comp, psicyc\_comp, risk\_assess}

∑2: {lock\_doors, door\_lock}

V: risk = N;

Ʌ: Transition specifications

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