Part 1

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

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

Σ2 = {*init\_err\_msg, idle\_err\_msg, moni\_err\_msg*}

q0 : *dormant*

V = *retry:* N0

Λ: Transition specifications

1. ------> dormant

2. dormant ----------------------------start-----------------------------------> init

3. dormant -----------------------------kill------------------------------------> final

4. init ----------------------------------------init\_ok----------------------------> idle

5. init --------------------------------------kill------------------------------------> final

6. init -------------------------init\_crash / init\_err\_msg--------------------> error\_diagnosis

7. idle ---------------------------begin\_monitoring---------------------------> monitoring

8. idle -------------------------idle\_crash/idle\_err\_msg---------------------> error\_diagnosis

9. idle -----------------------------------------kill----------------------------------> final

10. monitoring -------------monitor\_crash/moni\_err\_msg----------------> error\_diagnosis

11. monitoring --------------------------------kill----------------------------------> final

12. safe\_shutdown ---------------------------sleep-----------------------------> dormant

13. safe\_shutdown ---------------------------------kill--------------------------> final

14. error\_diagnosis ----------retry\_init [retry<3] / retry++----------------> init

15. error\_diagnosis ----------[retry>3] shutdown----------------------------> safe\_shutdown

16. error\_diagnosis --------------------idle\_rescue-----------------------------> idle

17. error\_diagnosis ---------------------moni\_rescue---------------------------> monitoring

18. error\_diagnosis -------------------------------kill-------------------------------> final

Part 2

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

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

Σ2 = {}

q0 : *boot\_hw*

V =

Λ: Transition specifications

1. ------> boot\_hw

1. boot\_hw ---------------------------hw\_ok-----------------------------------> senchk

2. senchk -----------------------------senok------------------------------------> tchk

2. tchk -----------------------------------t\_ok-----------------------------------> psichk

3. psichk ------------------------------ psi\_ok----------------------------------> ready

Part 3

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

Σ1 = {*no\_contagion, after\_100ms, contagion\_alert, purge\_succ*}

Σ2 = {FACILITY\_CRIT\_MESG}

q0 : *monidle*

V = *inlockdown* : Boolean.

Λ: Transition specifications

1. ------> monidle

2. monidle ---------------------------no\_contagion---------------------------------------------> regulate\_environment

3. regulate\_environment ------------after\_100ms------------------------------------------------> monidle

4. monidle -----contagion\_alert / (FACILITY\_CRIT\_MESG ; inlockdown = true)-----------> lockdown

5. lockdown -----------------purge\_succ / inlockdown = false -----------------------------------> monidle

6. monitoring --------monitor\_crash [inlockdown == true] / moni\_err\_msg-------------> monitoring

Part 4

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

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

Σ2 = {*lock\_doors*, *unlock\_doors*}

q0 : *prep\_vpurge*

V = *risk* : R.

Λ: Transition specifications

1. ------> prep\_vpurge

2. prep\_vpurge ---------------initiate\_purge / lock\_doors -------------------> alt\_temp

3. prep\_vpurge ---------------initiate\_purge / lock\_doors -------------------> alt\_psi

4. alt\_temp ----------------------------tcyc\_comp----------------------------------> risk\_assess

5. alt\_psi -----------------------------psicyc\_comp----------------------------------> risk\_assess

6. risk\_assess -----------------------[risk >= 0.01]----------------------------------> prep\_vpurge

7. risk\_assess -------------------[risk < 0.01] / unlock\_doors --------------------> safe\_status

8. safe\_status-----------------------------------------------------------------------------> final

Part 5

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

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

Σ2 = {}

q0 : *error\_rcv.*

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

Λ: Transition specifications

1. ------> error\_rcv

2. error\_rcv --------------- [err\_protocol\_def == false] -------------------> reset\_module\_data

3. error\_rcv ----------------[err\_protocol\_def == true]---------------------> applicable\_rescue

4. reset\_module\_data ---------------reset\_to\_stable-----------------------> final

5. applicable\_rescue ----------------apply\_protocol\_rescues--------------> final