The EFSM is the tuple S = (Q, Σ1, Σ2, q0, V, Λ),

where

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

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

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

q0 : dormant

V : retry = {0, 1,2,3}

Λunrefined ={

1. → dormant

2. dormantfinal

3. dormantinit

4. initidle

5. initerror\_diagnosis

6. initfinal

7. idlemonitoring

8. idleerror\_diagnosis

9. idlefinal

10. monitoringfinal

11. monitoringerror\_diagnosis

12. error\_diagnosisfinal

13. error\_diagnosismonitoring

14. error\_diagnosisinit

15. error\_diagnosisidle

16. error\_diagnosissafe\_shutdown

17. safe\_shutdownfinal

18. safe\_shutdown

}

The EFSM of the refined init state is the tuple 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 = {}

q0 : boot\_hw

V = {}

Λrefined ={

1. → boot\_hw
2. boot\_hwsenchk
3. senchktchk
4. tchkpsichk
5. psichkready

}

The EFSM of the refined monitoring state is the tuple S = (Q, Σ1, Σ2, q0, V, Λ),

where

Q = {monidle, regulate\_environment, lockdown}

Σ1 = {verify\_contagion, contagion\_alert,\_no\_contagion, after\_100ms, purge\_succ}

Σ2 = {inlockdown=false, inlockdown=true, set contagion}

q0 : monidle

V = {inlockdown{true, false}}

Λrefined ={

1. → monidle
2. monidleregulate\_environment
3. monidlelockdown
4. monidlemonidle
5. regulate\_environmentmonidle
6. lockdownmonidle

}

The EFSM of the refined lockdown state is the tuple S = (Q, Σ1, Σ2, q0, V, Λ),

where

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

Σ1 = {initiate\_purge, tcyc\_comp,\_psicyc\_comp, risk\_action, evaluate\_risk, perform\_alteration}

Σ2 = {lock\_doors, unlock\_doors, set risk}

q0 : prep\_vpurge

V = {risk}

Λrefined ={

1. → prep\_vpurge
2. prep\_vpurgealt\_temp
3. prep\_vpurgealt\_psi
4. alt\_tempalt\_temp
5. alt\_temprisk\_assess
6. alt\_psialt\_psi
7. alt\_psirisk\_assess
8. risk\_assessrisk\_assess
9. risk\_assesssafe\_status
10. risk\_assessprep\_vpurge

}

The EFSM of the refined error\_diagnosis state is the tuple S = (Q, Σ1, Σ2, q0, V, Λ),

where

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

Σ1 = {protocol\_search, protocol\_event, apply\_protocol\_rescue, reset\_to\_stable }

Σ2 = {set err\_protocol\_def}

q0 : error\_rcv

V = {err\_protocol\_def}

Λrefined ={

1. →error\_rcv
2. error\_rcverror\_rcv
3. error\_rcvapplicable\_rescue
4. error\_rcvreset\_module\_data
5. applicable\_rescuefinal
6. reset\_module\_datafinal

}