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 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, FACILITY\_CRIT\_MESG}

q0 : monidle

V = {inlockdown{true, false}}

Λrefined ={

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

}