**Formal Specifications**

Overall Safety Critical Room

S = (Q, ∑1, ∑2, q0, ∨, ∧)

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

∑1 = {start, kill, init\_ok, init\_crash, retry\_init, begin\_monitoring, idle\_crash, idle\_rescue, monitor\_crash, moni\_rescue, shutdown, sleep}

∑2 = {retry++, init\_err\_msg, idle\_err\_msg, moni\_err\_msg}

q0 : dormant

∨: retry: N0

∧: Transition specifications

1. 🡪 dormant
2. dormant start init
3. dormant kill exit
4. init init\_ok idle
5. init init\_crash/init\_err\_msg error\_diagnosis
6. idle begin\_monitoring monitoring
7. idle idle\_crash/idle\_err\_msg error\_diagnosis
8. monitoring monitor\_crash/moni\_err\_msg error\_diagnosis
9. error\_diagnosis retry\_init[retry < 3]/ retry++ init
10. error\_diagnosis shutdown[retry >= 3] safe\_shutdown
11. safe\_shutdown sleep dormant
12. error\_diagnosis idle\_rescue idle
13. error\_diagnosis moni\_rescue monitor

Refine Init

S = (Q, ∑1, ∑2, q0, ∨, ∧)

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

∑1 = {hw\_ok, senok, t\_ok, psi\_ok }

∑2 = { }

q0 : boot\_hw

∨: {}

∧: Transition specifications

1. 🡪 boot\_hw
2. boot\_hw hw\_ok senchk
3. senchk senok tchk
4. tchk t\_ok psichk
5. psichk psi\_ok ready

Refine Monitor

S = (Q, ∑1, ∑2, q0, ∨, ∧)

Q = {monidle, regulate\_environment, lockdown }

∑1 = {no\_contagion, after\_100ms, contagion\_alert, purge\_succ }

∑2 = {retry++, init\_err\_msg, idle\_err\_msg, moni\_err\_msg}

q0 : dormant

∨: inlockdown: Boolean

∧: Transition specifications

1. 🡪 monidle
2. monidle no\_contagion regulate\_environment
3. monidle contagion\_alert/ (FACILITY\_CRIT\_MESG; inlockdown=true) lockdown
4. regulate\_environment after\_100ms monidle
5. lockdown purge\_succ/inlockdown=false monidle
6. monitoring monitor\_crash[!inlockdown]/moni\_err\_msg error\_diagnosis

Refine Lockdown

S = (Q, ∑1, ∑2, q0, ∨, ∧)

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

∑1 = {initiate\_purge, psicyc\_comp, tcyc\_comp }

∑2 = {lock\_doors, unlock\_doors}

q0 : prep\_vpurge

∨: risk: N0

∧: Transition specifications

1. 🡪 prep\_vpurge
2. prep\_vpurge initiate\_purge/lock\_doors alt\_psi
3. prep\_vpurge initiate\_purge/lock\_doors alt\_temp
4. alt\_psi psicyc\_comp risk\_assess
5. alt\_temp tcyc\_comp risk\_assess
6. risk\_assess [risk < 0.01]/ unlock\_doors safe\_status
7. risk\_assess [risk >= 0.01] prep\_vpurge
8. safe\_status final

Refine Error\_Diagnosis

S = (Q, ∑1, ∑2, q0, ∨, ∧)

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

∑1 = {apply\_protocol\_rescue, reset\_to\_stable}

∑2 = { }

q0 : error\_rcv

∨: error\_protocol\_def: Boolean

∧: Transition specifications

1. 🡪 error\_rcv
2. error\_rcv [error\_protocol\_def] applicable\_rescue
3. error\_rcv [!error\_protocol\_def] reset\_module\_data
4. applicable\_rescue apply\_protocol\_rescue exit
5. reset\_module\_data reset\_to\_protocol exit