**Safety Critical System**

Q = {dormant, safe\_shutdown, init, idle, monitoring, error\_diagnosis}  
Σ1 = {kill, sleep, start, init\_ok, begin\_monitoring, idle\_rescue, idle\_crash, retry\_init, monitor\_crash, monitor\_rescue, init\_crash, shutdown}  
Σ2 = {broadcast idle\_err\_msg, retry++, broadcast moni\_err\_msg, broadcast init\_err\_msg, system clean up}  
q0 : dormant  
Ѵ : retry : ℕ0; inlockdown : boolean.  
Λ : Transition specifications

1.   
2.   
3.   
4.   
5.   
6.   
7.   
8.   
9.   
10.   
11.   
12.   
13.

**init**

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

Σ1 = {hw\_ok, senok, t\_ok, psi\_ok}

Σ2 = {}

q0 : boot\_hw

Ѵ = {}

Λ: Transition specifications

1.

2.

3.

4.

5.

**lockdown**

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

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

Σ2 = {lock\_doors, unlock\_doors}

q0 : prep\_vpurge

Ѵ : risk: percentage

Λ : Transition specifications

1.

2.

3.

4.

5.

6.

7.

8.

**error\_diagnosis**

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

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

Σ2 = { }

q0 : error\_rcv

Ѵ : err\_protocol\_def: Boolean

Λ : Transition specifications

1.

2.

3.

4.

5.