Roberto Ruffolo-Benavides (26974732)
Christiano Bianchet (27039573)

Formal Specifications

Overall

$S = (\, Q,\ \Sigma_1,\ \Sigma_2, q_0, V, \Lambda)$ where

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

$\Sigma_1\ = \{start,\ init\_ok,\ begin\_monitoring,\ init\_crash,\ kill, retry\_init,\ idle\_crash,$
$\quad idle\_rescue, monitor\_crash,\ moni\_rescue,\ shutdown,\ sleep\}$

$\Sigma_2 = \{init\_err\_msg,\ idle\_err\_msg,\ moni\_err\_msg\}$

$q_0\ : dormant$

$V\ : retry : N_0$

$\Lambda\ : Transitions\ Specifications$

$1.\ \ \rightarrow dormant$

$2.\ dormant \text{---} start \rightarrow init$

$3.\ dormant \text{---} kill \rightarrow final$

$4.\ init \text{---} init\_ok \rightarrow idle$

$5.\ init \text{---} init\_crash / init\_err\_msg \rightarrow error\_diagnosis$

$6.\ idle \text{---} begin\_monitoring \rightarrow monitoring$

$7.\ idle \text{---} idle\_crash / idle\_err\_msg \rightarrow error\_diagnosis$

$8.\ monitoring \text{---} monitor\_crash / moni\_err\_msg \rightarrow error\_diagnosis$

$9.\ error\_diagnosis \text{---} retry\_init[rety < 3] / retry{+}{+}\ \ \rightarrow init$

$10.\ error\_diagnosis \text{---} idle\_rescue \rightarrow idle$

$11.\ error\_diagnosis \text{---} moni\_rescue \rightarrow monitoring$

$12\ .error\_diagnosis \text{---} shutdown[retry \geq 3] \rightarrow safe\_shutdown$

$13.\ safe\_shutdown \text{---} sleep \rightarrow dormant$

Init

$S = (\, Q,\ \Sigma_1,\ \Sigma_2,\ q_0, V, \Lambda)$ where

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

$\Sigma_1\ = \{hw\_ok,\ sen\_ok,\ t\_ok,\ psi\_ok\}$

$\Sigma_2\ = \{\}$

$q_0 :\ boot\_hw$

$V :$

$\Lambda : Transitions\ Specifications$

1. $\rightarrow boot\_hw$
2. $boot\_hw --- hw\_ok \rightarrow senchk$
3. $senchk --- sen\_ok \rightarrow tchk$
4. $tchk --- t\_ok \rightarrow psichk$
5. $psichk --- psi\_ok \rightarrow ready$

Monitoring

$S = (\,Q,\ \Sigma_1,\ \Sigma_2,\ q_0, V, \Lambda)$ where

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

$\Sigma_1\ = \{after\_100ms,\ no\_contagion,\ contagion\_alert,\ purge\_succ\}$

$\Sigma_2\ = \{FACILITY\_CRIT\_MESG\}$

$q_0 :\ monidle$

$V :$

$\Lambda_{refined} : Transitions\ Specifications$

1. $\rightarrow monidle$
2. $monidle --- no\_contagion \rightarrow regulate\_environment$
3. $monidle --- contagion\_alert / FACILITY\_CRIT\_MESG,\ inlockdown\ =\ true \rightarrow lockdown$
4. $regulate\_environment --- after\_100ms \rightarrow monidle$
5. $lockdown --- purge\_succ / inlockdown\ =\ false \rightarrow monidle$

$\Lambda_{unrefined} : Transitions\ Specifications$

1. $monitoring --- monitor\_crash[!inlockdown]/moni\_err\_msg \rightarrow error\_diagnosis$

Error_Diagnosis

$S = (\,Q,\ \Sigma_1,\ \Sigma_2,\ q_0, V, \Lambda)$ where

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

$\Sigma_1\ = \{apply\_protocol\_rescues,\ reset\_to\_stable\}$

$\Sigma_2\ = \{\}$

$q_0 :\ error\_rcv$

$V :\ err\_protocol\_def :\ boolean$

$\Lambda : Transitions\ Specifications$

1. $\rightarrow error\_rcv$
2. $error\_rcv --- [error\_protocol\_def] \rightarrow applicable\_rescue$
3. $error\_rcv --- [!error\_protocol\_def] \rightarrow reset\_module\_data$
4. $applicable\_rescue --- apply\_protocol\_rescues \rightarrow final$
5. $reset\_module\_data --- reset\_to\_stable \rightarrow final$

Lockdown

$S = (\, Q, \Sigma_1, \Sigma_2, q_0, V, \Lambda)$ where

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

$\Sigma_1 = \{initiate\_purge, tcyc\_comp, psicyc\_comp\}$

$\Sigma_2 = \{lock\_doors, unlock\_doors\}$

$q_0 : prep\_vpurge$

$V : risk : R_+$

$\Lambda : Transitions\ Specifications$

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