Overview - Formal Specification

Q = {Dormant,Init,Idle,Monitoring,Error Diagnosis,Safe Shutdown}

Σ_1= {start,init_ok,begin_monitoring,init_crash,idle_crash,monitor_crash,retry_init,idle,rescue,moni_rescue,shutdown,sleep, kill}

Σ_2= { init_error_msg,idle_err_msg,moni_err_msg, retry++, load_drivers, confirm_drivers, begin_experiments, log_info, graceful_shutdown, moni_error_protocol, idle_error_protocol, turn_off, retry = 0 }

q_0 = Dormant

$\vee$: retry: $\mathbb{N}_0$; inlockdown = { true, false }

$\wedge$: Transitions specifications

1. —➤ Dormant
2. Dormant $\xrightarrow{\text{kill}}$ Exit
3. Dormant $\xrightarrow{\text{start / load\_drivers}}$ Init
4. Init $\xrightarrow{\text{init\_ok / confirm\_drivers}}$ Idle
5. Init $\xrightarrow{\text{init\_crash / (log\_info ; init\_err\_msg)}}$ Error Diagnosis
6. Idle $\xrightarrow{\text{begin\_monitoring / begin\_experiments}}$ Monitoring
7. Idle $\xrightarrow{\text{idle\_crash / idle\_err\_msg}}$ Error Diagnosis
8. Monitoring $\xrightarrow{\text{monitor\_crash [inlockdown=false] / moni\_err\_msg}}$ Error Diagnosis
9. Error Diagnosis $\xrightarrow{\text{retry\_init [retry<3] / retry++}}$ Init
10. Error Diagnosis $\xrightarrow{\text{idle\_rescue / idle\_error\_protocol}}$ Idle
11. Error Diagnosis $\xrightarrow{\text{moni\_rescue / moni\_error\_protocol}}$ Monitoring
12. Error Diagnosis $\xrightarrow{\text{shutdown [retry >= 3] / graceful\_shutdown}}$ Safe Shutdown

13. Safe Shutdown $\xrightarrow{\text{sleep}}$ Dormant

Init - Formal Specification

Q = {boot_hw, senchk, tchk, psychk, ready}

Σ_1**=** {hw_ok, senok, t_ok, psy_ok}

Σ_2**=** {}

$\mathbf{q_0}$ **=** boot_hw

⋁: {}

⋀: Transitions specifications

1. $\longrightarrow$ boot_hw
2. boot_hw $\xrightarrow{\text{hw\_ok}}$ senchk
3. senchk $\xrightarrow{\text{senok}}$ tchk
4. tchk $\xrightarrow{\text{t\_ok}}$ psychk
5. psychk $\xrightarrow{\text{psi\_ok}}$ ready

Monitoring - Formal Specification

Q = {monidle, regulate_environment, lockdown}

Σ_1**=** {no_contagion, after_100ms, contagion_alert, purge_succ}

Σ_2**=** {FACILITY_CRIT_MESG , inlockdown = false, inlockdown = true}

$\mathbf{q_0}$ **=** monidle

⋁: inlockdown ={ true, false }

Λ: Transitions specifications

1. $\longrightarrow$ monidle
2. monidle $\xrightarrow{\text{no\_contagion}}$ regulate_environment
3. regulate_environment $\xrightarrow{\text{after\_100ms}}$ monidle
4. regulate_envvironment $\xrightarrow{\text{contagion\_alert / (FACILITY\_CRIT\_MESG ; inlockdown = true)}}$ lockdown
5. lockdown $\xrightarrow{\text{purge\_succ / inlockdown = false}}$ monidle

Error Diagnosis - Formal Specification

Q = { error_rcv, reset_module_data, applicable_rescue }

Σ_1**=** {reset_to_stable, apply_protocol_rescues}

Σ_2**=** {}

q_0 = error_rcv

V: error_protocol_def = { true, false }

Λ: Transitions specifications

1. $\longrightarrow$ error_rcv
2. error_rcv $\xrightarrow{\text{[error\_protocol\_def = true]}}$ applicable_rescue
3. error_rcv $\xrightarrow{\text{[error\_protocol\_def = false]}}$ reset_module_data
4. applicable_rescue $\xrightarrow{\text{apply\_protocol\_rescues}}$ exit
5. reset_module_data $\xrightarrow{\text{reset\_to\_stable}}$ exit

Lockdown - Formal Specification

Q = { prep_vpurge, alt_temp, alt_psy, risk_assess, safe_status }

Σ_1= { initiate_purge, tcyc_comp, psicyc_comp }

Σ_2= {lock_doors, unlock_doors }

q_0 = prep_vpurge

$\vee$: risk: $\mathbb{N}_0$

$\wedge$: Transitions specifications

6. $\longrightarrow$ prep_vpurge
7. prep_vpurge $\xrightarrow{\text{initiate\_purge / lock\_doors}}$ alt_temp
8. alt_temp $\xrightarrow{\text{tcyc\_comp}}$ risk_assess
9. prep_vpurge $\xrightarrow{\text{initiate\_purge / lock\_doors}}$ alt_psy
10. alt_psy $\xrightarrow{\text{psicyc\_comp}}$ risk_assess
11. risk_assess $\xrightarrow{[\ \text{risk} > 1\%\ ]}$ prep_vpurge
12. risk_assess $\xrightarrow{[\ \text{risk} < 1\%\ ]\ \text{/ unlock\_doors}}$ safe_status
13. safe_status $\xrightarrow{\qquad\qquad}$ exit