MACHINE M_PartProc_Trans
REFINES M_Part_Trans
SEES C_Part_Proc_Trans
VARIABLES

partition_mode
processes
processes_of_partition
process_state
processes_of_cores
finished_core
location_of_service
create_process_parm

INVARIANTS

inv_prcos: $processes \in \mathbb{P}(PROCESSES)$

inv_proc_of_part: $processes\_of\_partition \in processes \pfun PARTITIONS$

inv_proc_state: $process\_state \in processes \pfun PROCESS\_STATES$

inv_runreadysuspfaltproc_onlyin_normal:
$\forall part\cdot(part \in PARTITIONS \land partition\_mode(part) \neq PM\_NORMAL \Rightarrow$
$\forall proc\cdot(proc \in (processes\_of\_partition^{-1}[\{part\}]\cap dom(process\_state))\land process\_state(proc) \in PROCESS\_STATES=$

$process\_state(proc) \neq PS\_Ready \land process\_state(proc) \neq PS\_Running \land process\_state(proc) \neq PS\_Suspend \land process\_state(proc) \neq PS\_Faulted))$

inv_runreadysuspfaltproc_imply_norl:
$\forall proc\cdot(proc \in processes\land proc \in (dom(process\_state)\cap dom(processes\_of\_partition))\land(process\_state(proc) = PS\_Ready\lor process\_state(proc) = PS\_Running\lor process\_state(proc) = PS\_Suspend\lor process\_state(proc) = PS\_Faulted) \Rightarrow$
$partition\_mode(processes\_of\_partition(proc)) = PM\_NORMAL)$

inv_noproc_imply_notnorl: $\forall part\cdot(part \in PARTITIONS \land part \in ran(processes\_of\_partition) \land finite(processes\_of\_partition^{-1}[\{part\}])\land card(processes\_of\_partition^{-1}[\{part\}]) = 0\Rightarrow partition\_mode(part) \neq PM\_NORMAL)$

inv_normal_imply_proc: $\forall part\cdot(part \in PARTITIONS \land partition\_mode(part) = PM\_NORMAL \land finite(processes\_of\_partition^{-1}[\{part\}])\Rightarrow part \in ran(processes\_of\_partition)\land card(processes\_of\_partition^{-1}[\{part\}$
$0)$

inv_idle_imply_not_includeproc_of_part: $\forall part\cdot(part \in PARTITIONS \land partition\_mode(part) = PM\_IDLE \Rightarrow part \notin ran(processes\_of\_partition))$

inv_procs_of_cores: $processes\_of\_cores \in processes \pfun CORES$

inv_cores_imply_procandpart: $\forall proc\cdot(proc \in processes \land proc \in dom(processes\_of\_cores) \land proc \in dom(processes\_of\_partition)\Rightarrow processes\_of\_cores(proc) \in Cores\_of\_Partition(processes\_of\_partition(proc)))$

inv_finished_core: $finished\_core \in CORES \rightarrow BOOL$

inv_loc_of_serv: $location\_of\_service \in CORES \pfun (Services \times Location)$

inv_local_service_and_finished_core: $\forall core, serv\cdot(core \in dom(location\_of\_service)\land serv \in Services\land location\_of\_service(core) \neq (serv \mapsto loc\_r) \Rightarrow finished\_core(core) = FALSE)$

inv_createproc_complete_imply_proc_state_totalfunc: $\forall core\cdot(core \in CORES\land core \in dom(location\_of\_service)\land finished\_core(core) = TRUE\land location\_of\_service(core) = (Create\_Process \mapsto loc\_r)\Rightarrow\forall proc\cdot(proc \in processes \Rightarrow process\_state(proc) \in PROCESS\_STATES))$

inv_create_proc_parm: ⟨theorem⟩ $create\_process\_parm \in CORES \pfun PROCESSES$

inv_local_and_create_proc_parm: $\forall core\cdot(core \in dom(location\_of\_service)\land(location\_of\_service(core) = (Create\_Process \mapsto loc\_i)\lor location\_of\_service(core) = (Create\_Process \mapsto loc\_1)\lor location\_of\_service(core) = (Create\_Process \mapsto loc\_1)) \Rightarrow core \in dom(create\_process\_parm))$

EVENTS

Initialisation ⟨extended⟩

begin

act001: $partition\_mode := PARTITIONS \times \{PM\_COLD\_START\}$
act101: $processes := \varnothing$

act102: $processes\_of\_partition := \varnothing$

act103: $process\_state := \varnothing$

act104: $processes\_of\_cores := \varnothing$

act105: $finished\_core := CORES \times \{TRUE\}$

act106: $location\_of\_service := \varnothing$

end

Event process_schedule ⟨ordinary⟩ $\widehat{=}$

any

part

proc

core

where

grd001: $part \in PARTITIONS$

grd002: $proc \in processes \cap dom(process\_state) \cap dom(processes\_of\_cores) \cap dom(processes\_of\_partition)$

grd003: $core \in CORES$

grd004: $processes\_of\_partition(proc) = part$

grd005: $core \in Cores\_of\_Partition(part)$

grd006: $processes\_of\_cores(proc) = core$

grd007: $partition\_mode(part) = PM\_NORMAL$

grd008: $process\_state(proc) = PS\_Ready \lor process\_state(proc) = PS\_Running$

then

skip

end

Event create_process_init ⟨ordinary⟩ $\widehat{=}$

any

part

proc

core

service

where

grd001: $part \in PARTITIONS$

grd002: $proc \in (PROCESSES \setminus processes)$

grd003: $core \in CORES$

grd004: $service \in Services$

grd005: $partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START$

grd006: $finished\_core(core) = TRUE$

grd007: $service = Create\_Process$

then

act001: $location\_of\_service(core) := service \mapsto loc\_i$

act002: $finished\_core(core) := FALSE$

act003: $processes := processes \cup \{proc\}$

act004: $processes\_of\_partition(proc) := part$

act005: $create\_process\_parm(core) := proc$

end

Event create_process_dormant ⟨ordinary⟩ $\widehat{=}$

any

part

proc

core

where

grd001: $part \in PARTITIONS$

grd002: $proc \in processes$

grd003: $core \in CORES \cap dom(location\_of\_service)$

grd004: $location\_of\_service(core) = Create\_Process \mapsto loc\_i$

grd005: $finished\_core(core) = FALSE$

grd006: $\neg(location\_of\_service(core) = Create\_Process \mapsto loc\_i \land finished\_core(core) = FALSE)$

grd007: $proc = create\_process\_parm(core)$

grd008: $processes\_of\_partition(proc) = part$

grd009: $partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START$

then

act001: $location\_of\_service(core) := Create\_Process \mapsto loc\_1$

act002: $process\_state(proc) := PS\_Dormant$

end

Event create_process_core ⟨ordinary⟩ $\widehat{=}$

any

part

proc

core

where

grd001: $part \in PARTITIONS$

grd002: $proc \in processes$

grd003: $core \in CORES \cap dom(location\_of\_service)$

grd004: $location\_of\_service(core) = Create\_Process \mapsto loc\_1$

grd005: $finished\_core(core) = FALSE$

grd006: $\neg(location\_of\_service(core) = Create\_Process \mapsto loc\_1 \land finished\_core(core) = FALSE)$

grd007: $processes\_of\_partition(proc) = part$

grd008: $process\_state(proc) = PS\_Dormant$

grd009: $create\_process\_parm(core) = proc$

grd010: $partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START$

then

act001: $location\_of\_service(core) := Create\_Process \mapsto loc\_2$

act002: $processes\_of\_cores(proc) := core$

end

Event create_process_return ⟨ordinary⟩ $\widehat{=}$

any

part

proc

core

where

grd001: $part \in PARTITIONS$

grd002: $proc \in processes$

grd003: $core \in CORES \cap dom(location\_of\_service)$

grd004: $location\_of\_service(core) = Create\_Process \mapsto loc\_2$

grd005: $finished\_core(core) = FALSE$

grd006: $\neg(location\_of\_service(core) = Create\_Process \mapsto loc\_2 \land finished\_core(core) = FALSE)$

grd007: $processes\_of\_partition(proc) = part$

grd008: $process\_state(proc) = PS\_Dormant$

grd009: $create\_process\_parm(core) = proc$

grd010: $partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START$

then

act001: $location\_of\_service(core) := Create\_Process \mapsto loc\_r$

act002: $finished\_core(core) := TRUE$

act003: $create\_process\_parm := \{core\} ⩤ create\_process\_parm$

end

Event partition_modetransition_to_idle ⟨ordinary⟩ $\widehat{=}$

refines partition_mode_transition

any

part

newm

procs

cores

where

grd001: $part \in PARTITIONS$

grd002: $newm \in PARTITION\_MODES$

grd101: $procs = processes\_of\_partition^{-1}[\{part\}]$

grd102: $cores \in \mathbb{P}_1\,(CORES)$

grd103: $partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START \lor partition\_mode(part) = PM\_NORMAL$

grd104: $newm = PM\_IDLE$

grd105: $cores = Cores\_of\_Partition(part)$

grd106: $\forall core \cdot (core \in (Cores\_of\_Partition(part) \cap dom(finished\_core)) \Rightarrow finished\_core(core) = TRUE)$

then

act001: $partition\_mode(part) := newm$

act101: $processes := processes \setminus procs$

act102: $process\_state := procs \domsub process\_state$

act103: $processes\_of\_partition := procs \domsub processes\_of\_partition$

act104: $processes\_of\_cores := procs \domsub processes\_of\_cores$

end

Event partition_modetransition_to_normal_init ⟨ordinary⟩ $\widehat{=}$

any

part

core

service

where

grd001: $part \in PARTITIONS$

grd002: $core \in CORES$

grd003: $service \in Services$

grd004: $partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START$

grd005: $finished\_core(core) = TRUE$

grd006: $service = Set\_Normal$

then

act001: $location\_of\_service(core) := service \mapsto loc\_i$

act002: $finished\_core(core) := FALSE$

end

Event partition_modetransition_to_normal_mode ⟨ordinary⟩ $\widehat{=}$

refines partition_mode_transition

any

part

newm

core

where

grd001: $part \in PARTITIONS$

grd002: $newm \in PARTITION\_MODES$

grd101: $core \in CORES \cap dom(location\_of\_service)$

grd102: $newm = PM\_NORMAL$

grd103: $finite(processes\_of\_partition^{-1}[\{part\}]) \land card(processes\_of\_partition^{-1}[\{part\}]) > 0$

grd104: $partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START$

grd105: $location\_of\_service(core) = Set\_Normal \mapsto loc\_i$

grd106: $finished\_core(core) = FALSE$

grd107: $\neg(location\_of\_service(core) = Set\_Normal \mapsto loc\_i \land finished\_core(core) = FALSE)$

then

act001: $location\_of\_service(core) := Set\_Normal \mapsto loc\_1$

act002: $partition\_mode(part) := newm$

end

Event partition_modetransition_to_normal_ready ⟨ordinary⟩ $\widehat{=}$

any

part

procs

procs2

procsstate
core

where

grd001: $part \in PARTITIONS$
grd002: $partition\_mode(part) = PM\_NORMAL$
grd003: $procs = processes\_of\_partition^{-1}[\{part\}] \cap process\_state^{-1}[\{PS\_Waiting\}]$
grd004: $procs2 = processes\_of\_partition^{-1}[\{part\}] \cap process\_state^{-1}[\{PS\_WaitandSuspend\}]$
grd005: $procsstate \in procs \rightarrow \{PS\_Waiting, PS\_Ready\}$
grd006: $core \in CORES \cap dom(location\_of\_service)$
grd007: $location\_of\_service(core) = Set\_Normal \mapsto loc\_1$
grd008: $finished\_core(core) = FALSE$
grd009: $\neg(location\_of\_service(core) = Set\_Normal \mapsto loc\_1 \land finished\_core(core) = FALSE)$

then

act001: $location\_of\_service(core) := Set\_Normal \mapsto loc\_2$
act002: $process\_state := (process\_state \mathbin{<\!\!+} procsstate) \mathbin{<\!\!+} (procs2 \times \{PS\_Suspend\})$

end

Event partition_modetransition_to_normal_return ⟨ordinary⟩ $\widehat{=}$

any

part
core

where

grd001: $part \in PARTITIONS$
grd002: $partition\_mode(part) = PM\_NORMAL$
grd003: $core \in CORES \cap dom(location\_of\_service)$
grd004: $location\_of\_service(core) = Set\_Normal \mapsto loc\_2$
grd005: $finished\_core(core) = FALSE$
grd006: $\neg(location\_of\_service(core) = Set\_Normal \mapsto loc\_2 \land finished\_core(core) = FALSE)$

then

act001: $location\_of\_service(core) := Set\_Normal \mapsto loc\_r$
act002: $finished\_core(core) := TRUE$

end

Event partition_modetransition_to_coldstart ⟨ordinary⟩ $\widehat{=}$

refines partition_mode_transition

any

part
newm
procs
cores

where

grd001: $part \in PARTITIONS$
grd002: $newm \in PARTITION\_MODES$
grd101: $cores \in \mathbb{P}_1(CORES)$
grd102: $newm = PM\_COLD\_START$
grd103: $partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START \lor partition\_mode(part) = PM\_NORMAL$
grd107: $part \in ran(processes\_of\_partition)$
grd104: $procs = processes\_of\_partition^{-1}[\{part\}]$
grd105: $cores = Cores\_of\_Partition(part)$
grd106: $\forall core\cdot(core \in (Cores\_of\_Partition(part) \cap dom(finished\_core)) \Rightarrow finished\_core(core) = TRUE)$

then

act001: $partition\_mode(part) := newm$
act101: $processes := processes \setminus procs$
act102: $process\_state := procs \mathbin{\lhd\!\!\!-} process\_state$
act103: $processes\_of\_partition := procs \mathbin{\lhd\!\!\!-} processes\_of\_partition$
act104: $processes\_of\_cores := procs \mathbin{\lhd\!\!\!-} processes\_of\_cores$

end

Event partition_modetransition_to_warmstart ⟨ordinary⟩ $\widehat{=}$

refines partition_mode_transition

any

part
newm
procs
cores

where

grd001: $part \in PARTITIONS$
grd002: $newm \in PARTITION\_MODES$
grd101: $cores \in \mathbb{P}_1\,(CORES)$
grd102: $newm = PM\_WARM\_START$
grd103: $partition\_mode(part) = PM\_WARM\_START \lor partition\_mode(part) = PM\_NORMAL$
grd104: $procs = processes\_of\_partition^{-1}[\{part\}]$
grd105: $cores = Cores\_of\_Partition(part)$
grd106: $\forall core\cdot(core \in (Cores\_of\_Partition(part) \cap dom(finished\_core)) \Rightarrow finished\_core(core) = TRUE)$

then

act001: $partition\_mode(part) := newm$
act101: $processes := processes \setminus procs$
act102: $process\_state := procs \mathbin{⩤} process\_state$
act103: $processes\_of\_partition := procs \mathbin{⩤} processes\_of\_partition$
act104: $processes\_of\_cores := procs \mathbin{⩤} processes\_of\_cores$

end

Event partition_modetransition_idle_to_warmstart ⟨ordinary⟩ $\widehat{=}$
refines partition_mode_transition

any

part
newm
cores

where

grd001: $part \in PARTITIONS$
grd002: $newm \in PARTITION\_MODES$
grd101: $cores \in \mathbb{P}_1\,(CORES)$
grd102: $newm = PM\_WARM\_START$
grd103: $partition\_mode(part) = PM\_IDLE$
grd104: $cores = Cores\_of\_Partition(part)$
grd105: $\forall core\cdot(core \in (Cores\_of\_Partition(part) \cap dom(finished\_core)) \Rightarrow finished\_core(core) = TRUE)$

then

act001: $partition\_mode(part) := newm$

end

Event partition_modetransition_idle_to_coldstart ⟨ordinary⟩ $\widehat{=}$
refines partition_mode_transition

any

part
newm
cores

where

grd001: $part \in PARTITIONS$
grd002: $newm \in PARTITION\_MODES$
grd101: $cores \in \mathbb{P}_1\,(CORES)$
grd102: $newm = PM\_COLD\_START$
grd103: $partition\_mode(part) = PM\_IDLE$
grd104: $cores = Cores\_of\_Partition(part)$
grd105: $\forall core\cdot(core \in (Cores\_of\_Partition(part) \cap dom(finished\_core)) \Rightarrow finished\_core(core) = TRUE)$

then

act001: $partition\_mode(part) := newm$

end

Event process_state_transition ⟨ordinary⟩ $\widehat{=}$

any

part

proc

newstate

core

where

grd001: $part \in PARTITIONS$

grd002: $proc \in processes \cap dom(processes\_of\_partition) \cap dom(process\_state)$

grd003: $newstate \in PROCESS\_STATES$

grd004: $core \in CORES$

grd005: $processes\_of\_partition(proc) = part$

grd006: $partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START \lor partition\_mode(part) = PM\_NORMAL$

grd007: $((partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START) \land process\_state(proc) = PS\_Dormant) \Rightarrow newstate = PS\_Waiting$

grd008: $((partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START) \land process\_state(proc) = PS\_Waiting) \Rightarrow (newstate = PS\_Dormant \lor newstate = PS\_WaitandSuspend)$

grd009: $((partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START) \land process\_state(proc) = PS\_WaitandSuspend) \Rightarrow (newstate = PS\_Waiting \lor newstate = PS\_Dormant)$

grd010: $(partition\_mode(part) = PM\_NORMAL \land process\_state(proc) = PS\_Dormant) \Rightarrow (newstate = PS\_Ready \lor newstate = PS\_Waiting)$

grd011: $(partition\_mode(part) = PM\_NORMAL \land process\_state(proc) = PS\_Ready) \Rightarrow (newstate = PS\_Dormant \lor newstate = PS\_Suspend)$

grd012: $(partition\_mode(part) = PM\_NORMAL \land process\_state(proc) = PS\_Waiting) \Rightarrow (newstate = PS\_Dormant \lor newstate = PS\_Ready \lor newstate = PS\_WaitandSuspend)$

grd013: $(partition\_mode(part) = PM\_NORMAL \land process\_state(proc) = PS\_Suspend) \Rightarrow (newstate = PS\_Dormant \lor newstate = PS\_Ready)$

grd014: $(partition\_mode(part) = PM\_NORMAL \land process\_state(proc) = PS\_WaitandSuspend) \Rightarrow (newstate = PS\_Dormant \lor newstate = PS\_Waiting \lor newstate = PS\_Suspend)$

grd015: $(partition\_mode(part) = PM\_NORMAL \land process\_state(proc) = PS\_Running) \Rightarrow (newstate = PS\_Dormant \lor newstate = PS\_Ready \lor newstate = PS\_Running \lor newstate = PS\_Waiting \lor newstate = PS\_Suspend \lor newstate = PS\_Faulted)$

grd016: $(partition\_mode(part) = PM\_NORMAL \land process\_state(proc) = PS\_Faulted) \Rightarrow newstate = PS\_Dormant$

then

act001: $process\_state(proc) := newstate$

end

Event process_state_transition2 ⟨ordinary⟩ $\widehat{=}$

any

part

procs

newstates

core

where

grd001: $part \in PARTITIONS$

grd002: $procs \subseteq processes \cap dom(process\_state)$

grd003: $newstates \in procs \rightarrow PROCESS\_STATES$

grd004: $core \in CORES$

grd005: $procs \subseteq processes\_of\_partition^{-1}[\{part\}]$

grd006: $partition\_mode(part) = PM\_NORMAL \lor partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START$

grd007: $\forall proc \cdot ((proc \in procs \land (partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START) \land process\_state(proc) = PS\_Dormant) \Rightarrow newstates(proc) = PS\_Waiting)$

grd008: $\forall proc \cdot ((proc \in procs \land (partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START) \land process\_state(proc) = PS\_Waiting) \Rightarrow (newstates(proc) = PS\_Dormant \lor newstates(proc) = PS\_WaitandSuspend))$

grd009: $\forall proc\cdot((proc \in procs \land (partition\_mode(part) = PM\_COLD\_START \lor partition\_mode(part) = PM\_WARM\_START) \land process\_state(proc) = PS\_WaitandSuspend) \Rightarrow (newstates(proc) = PS\_Waiting \lor newstates(proc) = PS\_Dormant))$

grd010: $\forall proc\cdot(proc \in procs \land (partition\_mode(part) = PM\_NORMAL \land process\_state(proc) = PS\_Dormant) \Rightarrow (newstates(proc) = PS\_Ready \lor newstates(proc) = PS\_Waiting))$

grd011: $\forall proc\cdot(proc \in procs \land (partition\_mode(part) = PM\_NORMAL \land process\_state(proc) = PS\_Ready) \Rightarrow (newstates(proc) = PS\_Dormant \lor newstates(proc) = PS\_Suspend))$

grd012: $\forall proc\cdot(proc \in procs \land (partition\_mode(part) = PM\_NORMAL \land process\_state(proc) = PS\_Waiting) \Rightarrow (newstates(proc) = PS\_Dormant \lor newstates(proc) = PS\_Ready \lor newstates(proc) = PS\_WaitandSuspend))$

grd013: $\forall proc\cdot(proc \in procs \land (partition\_mode(part) = PM\_NORMAL \land process\_state(proc) = PS\_Suspend) \Rightarrow (newstates(proc) = PS\_Dormant \lor newstates(proc) = PS\_Ready))$

grd014: $\forall proc\cdot(proc \in procs \land (partition\_mode(part) = PM\_NORMAL \land process\_state(proc) = PS\_WaitandSuspend) \Rightarrow (newstates(proc) = PS\_Dormant \lor newstates(proc) = PS\_Waiting \lor newstates(proc) = PS\_Suspend))$

grd015: $\forall proc\cdot(proc \in procs \land (partition\_mode(part) = PM\_NORMAL \land process\_state(proc) = PS\_Running) \Rightarrow (newstates(proc) = PS\_Dormant \lor newstates(proc) = PS\_Ready \lor newstates(proc) = PS\_Running \lor newstates(proc) = PS\_Waiting \lor newstates(proc) = PS\_Suspend \lor newstates(proc) = PS\_Faulted))$

grd016: $\forall proc\cdot(proc \in procs \land (partition\_mode(part) = PM\_NORMAL \land process\_state(proc) = PS\_Faulted) \Rightarrow newstates(proc) = PS\_Dormant)$

then

act001: $process\_state := process\_state \mathbin{\lhd\mkern-9mu-} newstates$

end

END