```
machine Mach_HM refines Mach_IPC   sees Ctx_HM

variables processes processes_of_partition partition_mode process_state periodtype_of_process
          process_wait_type
          locklevel_of_partition
          startcondition_of_partition
          basepriority_of_process
          period_of_process
          timecapacity_of_process
          deadline_of_process
          currentpriority_of_process
          deadlinetime_of_process
          releasepoint_of_process
          delaytime_of_process
          current_partition
          current_process
          current_partition_flag
          current_process_flag
          clock_tick
          need_reschedule
          need_procresch
```

preempter_of_partition
timeout_trigger
errorhandler_of_partition
process_call_errorhandler
queuing_ports sampling_ports
RefreshPeriod_of_SamplingPorts
msgspace_of_samplingports
needtrans_of_sourcesamplingport
queue_of_queueingports quediscipline_of_queueingports
processes_waitingfor_queuingports
buffers blackboards semaphores events_ buffers_of_partition blackboards_of_partition semaphores_of_partition events_of_partition MaxMsgNum_of_Buffers queue_of_buffers processes_waitingfor_buffers quediscipline_of_buffers msgspace_of_blackboards emptyindicator_of_blackboards processes_waitingfor_blackboards MaxValue_of_Semaphores value_of_semaphores quediscipline_of_semaphores processes_waitingfor_semaphores state_of_events processes_waitingfor_events
used_messages
module_shutdown

invariants

@inv_module_shutdown module_shutdown∈BOOL

```
events
  event INITIALISATION extends INITIALISATION
    then
      @act701 module_shutdown ≔ FALSE
  end

  event create_error_handler extends create_process
    where
      @grd700 module_shutdown = FALSE
      @grd701 basepriority=MAX_PRIORITY_VALUE
      @grd702 part∉dom(errorhandler_of_partition)
  end

  event report_application_message
    where
      @grd700 module_shutdown = FALSE
  end

  event get_error_status
    where
```

```
        @grd700 module_shutdown = FALSE
        @grd01 current_partition_flag = TRUE ∧ current_process_flag = TRUE
        @grd02 current_partition∈dom(errorhandler_of_partition) ∧ current_process =
errorhandler_of_partition(current_partition)
        @grd03 current_process ∈ dom(process_call_errorhandler)
  end

  event hm_recoveryaction_shutdown_module
    any errcode part
    where
        @grd700 module_shutdown = FALSE
        @grd701 errcode∈SYSTEM_ERRORS
        @grd702 errcode∈dom(MultiPart_HM_Table(part))
        @grd703 errcode ↦ MLA_SHUTDOWN ∈ MultiPart_HM_Table(part)
    then
        @act701 module_shutdown≔TRUE
  end

  event hm_recoveryaction_reset_module
    any errcode part
    where
    @grd700 module_shutdown = FALSE
    @grd701 errcode∈SYSTEM_ERRORS
    @grd702 errcode∈dom(MultiPart_HM_Table(part))
    @grd703 errcode ↦ MLA_RESET ∈ MultiPart_HM_Table(part)
end

event hm_recoveryaction_ignore_module
  any errcode part
  where
    @grd700 module_shutdown = FALSE
    @grd701 errcode∈SYSTEM_ERRORS
    @grd702 errcode∈dom(MultiPart_HM_Table(part))
    @grd703 errcode ↦ MLA_IGNORE ∈ MultiPart_HM_Table(part)
end

event hm_recoveryaction_idle_partition extends set_partition_mode_to_idle
  any errcode
  where
    @grd700 module_shutdown = FALSE
    @grd701 errcode∈SYSTEM_ERRORS ∧ part∈PARTITIONS
    @grd703 (errcode∈dom(Partition_HM_Table(part)) ∧ ERROR_LEVEL_PARTITION2↦PLA_IDLE∈
dom(Partition_HM_Table(part)(errcode)))
              ∨ (part∉dom(errorhandler_of_partition)) ∨ (current_process = errorhandler_of_partition(part))
 end

 event hm_recoveryaction_coldstart_partition extends set_partition_mode_to_coldstart
   any errcode
   where
     @grd700 module_shutdown = FALSE
     @grd701 errcode∈SYSTEM_ERRORS ∧ part∈PARTITIONS
     @grd703 (errcode∈dom(Partition_HM_Table(part)) ∧ ERROR_LEVEL_PARTITION2↦PLA_COLD_START∈
dom(Partition_HM_Table(part)(errcode)))
              ∨ (part∉dom(errorhandler_of_partition)) ∨ (current_process = errorhandler_of_partition(part))
 end

 event hm_recoveryaction_warmstart_partition extends set_partition_mode_to_warmstart
   any errcode
   where
     @grd700 module_shutdown = FALSE
     @grd701 errcode∈SYSTEM_ERRORS
     @grd703 (errcode∈dom(Partition_HM_Table(part)) ∧ ERROR_LEVEL_PARTITION2↦PLA_WARM_START
∈dom(Partition_HM_Table(part)(errcode)))
```

```
                ∨ (part∉dom(errorhandler_of_partition)) ∨ (current_process = errorhandler_of_partition(part))
  end

  event hm_recoveryaction_ignore_partition
    any errcode part
    where
      @grd700 module_shutdown = FALSE
      @grd701 errcode∈SYSTEM_ERRORS ∧ part∈PARTITIONS
      @grd703 (errcode∈dom(Partition_HM_Table(part)) ∧ ERROR_LEVEL_PARTITION2↦PLA_IGNORE∈
dom(Partition_HM_Table(part)(errcode)))
                ∨ (part∉dom(errorhandler_of_partition)) ∨ (current_process = errorhandler_of_partition(part))
  end

  event hm_recoveryaction_errorhandler extends start_aperiodprocess_innormal
    any errcode
    where
      @grd700 module_shutdown = FALSE
      @grd701 errcode∈SYSTEM_ERRORS
      @grd702 (errcode∈dom(Partition_HM_Table(part)) ∧ ∃a·(a∈PARTITION_RECOVERY_ACTIONS ∧
ERROR_LEVEL_PROCESS↦a∈dom(Partition_HM_Table(part)(errcode)))   )
      @grd703 DEADLINE_MISSED∈ran(Partition_HM_Table(part)(errcode)) ⇒ (∃pc·(pc∈
processes_of_partition∼[{part}] ∧ pc∈dom(deadlinetime_of_process)∧clock_tick∗ONE_TICK_TIME >
deadlinetime_of_process(pc)))
      @grd704 part∈dom(errorhandler_of_partition)
      @grd705 current_process ≠ errorhandler_of_partition(part)
      @grd706 proc = errorhandler_of_partition(part)
  end

  event create_sampling_port extends create_sampling_port
    where
      @grd700 module_shutdown = FALSE
  end

  event write_sampling_message extends write_sampling_message
    where
      @grd700 module_shutdown = FALSE
  end

  event transfer_sampling_msg extends transfer_sampling_msg
    where
      @grd700 module_shutdown = FALSE
  end
```

```
event read_sampling_message extends read_sampling_message
  where
    @grd700 module_shutdown = FALSE
end

event get_sampling_port_id extends get_sampling_port_id
  where
    @grd700 module_shutdown = FALSE
end

event get_sampling_port_status extends get_sampling_port_status
  where
    @grd700 module_shutdown = FALSE
end

event create_queuing_port extends create_queuing_port
  where
    @grd700 module_shutdown = FALSE
end
```

```
event send_queuing_message extends send_queuing_message
  where
    @grd700 module_shutdown = FALSE
end

event send_queuing_message_needwait
extends send_queuing_message_needwait
  where
    @grd700 module_shutdown = FALSE
end

event transfer_queuing_msg extends transfer_queuing_msg
  where
    @grd700 module_shutdown = FALSE
end

event wakeup_waitproc_on_srcqueports
extends wakeup_waitproc_on_srcqueports
  where
    @grd700 module_shutdown = FALSE
end
```

```
event wakeup_waitproc_on_destqueports
extends wakeup_waitproc_on_destqueports
  where
    @grd700 module_shutdown = FALSE
end

event receive_queuing_message extends receive_queuing_message
  where
    @grd700 module_shutdown = FALSE
end

event receive_queuing_message_needwait
extends receive_queuing_message_needwait
  where
    @grd700 module_shutdown = FALSE
end

event get_queuing_port_id extends get_queuing_port_id
  where
    @grd700 module_shutdown = FALSE
```

```
end

event get_queuing_port_status extends get_queuing_port_status
  where
    @grd700 module_shutdown = FALSE
end

event clear_queuing_port extends clear_queuing_port
  where
    @grd700 module_shutdown = FALSE
end

event create_buffer extends create_buffer
  where
    @grd700 module_shutdown = FALSE
end

event send_buffer extends send_buffer
  where
    @grd700 module_shutdown = FALSE
end
```

```
event send_buffer_needwakeuprecvproc
extends send_buffer_needwakeuprecvproc
  where
    @grd700 module_shutdown = FALSE
end

event send_buffer_withfull
extends send_buffer_withfull
  where
    @grd700 module_shutdown = FALSE
end

event receive_buffer extends receive_buffer
  where
    @grd700 module_shutdown = FALSE
end

event receive_buffer_needwakeupsendproc
extends receive_buffer_needwakeupsendproc
  where
```

```
      @grd700 module_shutdown = FALSE
end

event receive_buffer_whenempty
extends receive_buffer_whenempty
   where
      @grd700 module_shutdown = FALSE
end

event get_buffer_id extends get_buffer_id
   where
      @grd700 module_shutdown = FALSE
end

event get_buffer_status extends get_buffer_status
   where
      @grd700 module_shutdown = FALSE
end

event create_blackboard extends create_blackboard
   where
```

```
    @grd700 module_shutdown = FALSE
end

event display_blackboard extends display_blackboard
  where
    @grd700 module_shutdown = FALSE
end

event display_blackboard_needwakeuprdprocs
extends display_blackboard_needwakeuprdprocs
  where
    @grd700 module_shutdown = FALSE
end

event read_blackboard extends read_blackboard
  where
    @grd700 module_shutdown = FALSE
end

event read_blackboard_whenempty
extends read_blackboard_whenempty
```

```
  where
    @grd700 module_shutdown = FALSE
end

event clear_blackboard extends clear_blackboard
  where
    @grd700 module_shutdown = FALSE
end

event get_blackboard_id extends get_blackboard_id
  where
    @grd700 module_shutdown = FALSE
end

event get_blackboard_status extends get_blackboard_status
  where
    @grd700 module_shutdown = FALSE
end

event create_semaphore extends create_semaphore
  where
```

```
    @grd700 module_shutdown = FALSE
end

event wait_semaphore extends wait_semaphore
  where
    @grd700 module_shutdown = FALSE
end

event wait_semahpore_whenzero
extends wait_semahpore_whenzero
  where
    @grd700 module_shutdown = FALSE
end

event signal_semaphore extends signal_semaphore
  where
    @grd700 module_shutdown = FALSE
end

event signal_semaphore_needwakeupproc
extends signal_semaphore_needwakeupproc
```

```
  where
    @grd700 module_shutdown = FALSE
end

event get_semaphore_id extends get_semaphore_id
  where
    @grd700 module_shutdown = FALSE
end

event get_semaphore_status extends get_semaphore_status
  where
    @grd700 module_shutdown = FALSE
end

event create_event extends create_event
  where
    @grd700 module_shutdown = FALSE
end

event set_event extends set_event
  where
```

```
    @grd700 module_shutdown = FALSE
end

event set_event_needwakeupprocs
extends set_event_needwakeupprocs
  where
    @grd700 module_shutdown = FALSE
end

event reset_event extends reset_event
  where
    @grd700 module_shutdown = FALSE
end

event wait_event extends wait_event
  where
    @grd700 module_shutdown = FALSE
end

event wait_event_whendown
extends wait_event_whendown
```

```
  where
    @grd700 module_shutdown = FALSE
end

event get_event_id extends get_event_id
  where
    @grd700 module_shutdown = FALSE
end

event get_event_status extends get_event_status
  where
    @grd700 module_shutdown = FALSE
end

event ticktock
extends ticktock
  where
    @grd700 module_shutdown = FALSE
end

event partition_schedule extends partition_schedule
```

```
  where
    @grd700 module_shutdown = FALSE
end

event process_schedule
extends process_schedule
  where
    @grd700 module_shutdown = FALSE
end

event run_errorhandler_preempter
extends run_errorhandler_preempter
  where
    @grd700 module_shutdown = FALSE
end

event get_partition_status extends get_partition_status
  where
    @grd700 module_shutdown = FALSE
end
```

```
event set_partition_mode_to_idle
extends set_partition_mode_to_idle
  where
    @grd700 module_shutdown = FALSE
end

event set_partition_mode_to_normal extends set_partition_mode_to_normal
  where
    @grd700 module_shutdown = FALSE
end

event set_partition_mode_to_coldstart extends set_partition_mode_to_coldstart
  where
    @grd700 module_shutdown = FALSE
end

event set_partition_mode_to_warmstart extends set_partition_mode_to_warmstart
  where
    @grd700 module_shutdown = FALSE
end
```

```
event get_process_id extends get_process_id
  where
    @grd700 module_shutdown = FALSE
end

event get_process_status extends get_process_status
  where
    @grd700 module_shutdown = FALSE
end

event create_process extends create_process
  where
    @grd700 module_shutdown = FALSE
end

event set_priority extends set_priority
  where
    @grd700 module_shutdown = FALSE
end

event suspend_self
```

```
extends suspend_self
  where
    @grd700 module_shutdown = FALSE
end

event suspend
extends suspend
  where
    @grd700 module_shutdown = FALSE
end

event resume
extends resume
  where
    @grd700 module_shutdown = FALSE
end

event stop_self extends stop_self
  where
    @grd700 module_shutdown = FALSE
end
```

```
event stop extends stop
  where
    @grd700 module_shutdown = FALSE
end

event stop_wf_qport extends stop_wf_qport
where
    @grd700 module_shutdown = FALSE
end

event stop_wf_buf extends stop_wf_buf
where
    @grd700 module_shutdown = FALSE
end

event stop_wf_sem extends stop_wf_sem
where
    @grd700 module_shutdown = FALSE
end
```

```
event stop_wf_bb extends stop_wf_bb
where
    @grd700 module_shutdown = FALSE
end

event stop_wf_evt extends stop_wf_evt
where
    @grd700 module_shutdown = FALSE
end

event start_aperiodprocess_instart
extends start_aperiodprocess_instart
  where
    @grd700 module_shutdown = FALSE
end

event start_aperiodprocess_innormal
extends start_aperiodprocess_innormal
  where
    @grd700 module_shutdown = FALSE
end
```

```
event start_periodprocess_instart
extends start_periodprocess_instart
  where
    @grd700 module_shutdown = FALSE
end

event start_periodprocess_innormal
extends start_periodprocess_innormal
  where
    @grd700 module_shutdown = FALSE
end

event delaystart_aperiodprocess_instart
extends delaystart_aperiodprocess_instart
  where
    @grd700 module_shutdown = FALSE
end

event delaystart_aperiodprocess_innormal
extends delaystart_aperiodprocess_innormal
```

```
  where
    @grd700 module_shutdown = FALSE
end

event delaystart_periodprocess_instart
extends delaystart_periodprocess_instart
  where
    @grd700 module_shutdown = FALSE
end

event delaystart_periodprocess_innormal
extends delaystart_periodprocess_innormal
  where
    @grd700 module_shutdown = FALSE
end

event lock_preemption extends lock_preemption
  where
    @grd700 module_shutdown = FALSE
end
```

```
event unlock_preemption extends unlock_preemption
  where
    @grd700 module_shutdown = FALSE
end

event get_my_id extends get_my_id
  where
    @grd700 module_shutdown = FALSE
end

event timed_wait extends timed_wait
  where
    @grd700 module_shutdown = FALSE
end

event period_wait extends period_wait
  where
    @grd700 module_shutdown = FALSE
end

event get_time extends get_time
```

```
  where
    @grd700 module_shutdown = FALSE
end

event replenish extends replenish
  where
    @grd700 module_shutdown = FALSE
end

event aperiodicprocess_finished extends aperiodicprocess_finished
  where
    @grd700 module_shutdown = FALSE
end

event periodicprocess_finished extends periodicprocess_finished
  where
    @grd700 module_shutdown = FALSE
end

event time_out
extends time_out
```

```
  where
      @grd700 module_shutdown = FALSE
end


event time_out_wf_qport extends time_out_wf_qport
where
      @grd700 module_shutdown = FALSE
end

event time_out_wf_buf extends time_out_wf_buf
where
      @grd700 module_shutdown = FALSE
end

event time_out_wf_sem extends time_out_wf_sem
where
      @grd700 module_shutdown = FALSE
end

event time_out_wf_bb extends time_out_wf_bb
```

```
where
    @grd700 module_shutdown = FALSE
end

event time_out_wf_evt extends time_out_wf_evt
where
    @grd700 module_shutdown = FALSE
end

event periodicproc_reach_releasepoint extends periodicproc_reach_releasepoint
  where
    @grd700 module_shutdown = FALSE
end

event coldstart_partition_fromidle extends coldstart_partition_fromidle
  where
    @grd700 module_shutdown = FALSE
end

event warmstart_partition_fromidle extends warmstart_partition_fromidle
  where
```

```
      @grd700 module_shutdown = FALSE
  end
end
```