```
context Ctx_HM
//* ************************************************
//     The Event-B model of ARINC 653 Part 1
//     Created by Yongwang Zhao ( zhaoyongwang@gmail.com)
//     National Key Laboratory of Software Development Environment (NLSDE)
//     School of Computer and Engineering, Beihang University,  Beijing, China
//     ***********************************************/
extends Ctx_IPC

sets
    SYSTEM_ERRORS
    MODULE_RECOVERY_ACTIONS
    PARTITION_RECOVERY_ACTIONS
    ERROR_LEVEL_MP  //Error levels for Multi-Partition HM table
    ERROR_LEVEL_P  //Error levels  for Partition HM table
    MODULE_STATES
    PROC_LEVEL_ERRORS

constants
    DEADLINE_MISSED APPLICATION_ERROR NUMERIC_ERROR ILLEGAL_REQUEST
    STACK_OVERFLOW MEMORY_VIOLATION  HARDWARE_FAULT POWER_FAILURE // Predefined ARINC 653
```

```
process level error codes

    PLA_IGNORE PLA_IDLE PLA_WARM_START   PLA_COLD_START //Error recovery actions to take when
partition level errors occur Type

    MLA_IGNORE  MLA_SHUTDOWN  MLA_RESET //Recovery action to take when error level is MODULE
    ERROR_LEVEL_MODULE  ERROR_LEVEL_PARTITION1    ERROR_LEVEL_PARTITION2
ERROR_LEVEL_PROCESS // types of error level

    Module_HM_Table
    MultiPart_HM_Table
    Partition_HM_Table

axioms
    @axm01 finite(SYSTEM_ERRORS)  ∧  card(SYSTEM_ERRORS)  > 0
    @axm02 partition(ERROR_LEVEL_MP,{ERROR_LEVEL_MODULE},{ERROR_LEVEL_PARTITION1})
    @axm03 partition(ERROR_LEVEL_P,{ERROR_LEVEL_PARTITION2},{ERROR_LEVEL_PROCESS})
    @axm04 partition(MODULE_RECOVERY_ACTIONS,{MLA_IGNORE},{MLA_SHUTDOWN},{MLA_RESET})
    @axm05
partition(PARTITION_RECOVERY_ACTIONS,{PLA_IGNORE},{PLA_IDLE},{PLA_WARM_START},{PLA_COLD_START})
```

```
    @axm06 finite(MODULE_STATES) ∧ card(MODULE_STATES) > 0
    @axm10
partition(PROC_LEVEL_ERRORS,{DEADLINE_MISSED},{APPLICATION_ERROR},{NUMERIC_ERROR},{ILLEGAL_REQUEST},{STACK_OVERFLOW},{MEMORY_VIOLATION},{HARDWARE_FAULT},{POWER_FAILURE})
    @axm07 Module_HM_Table∈SYSTEM_ERRORS⇸(MODULE_STATES × MODULE_RECOVERY_ACTIONS)
    @axm08 MultiPart_HM_Table∈PARTITIONS→(SYSTEM_ERRORS⇸MODULE_RECOVERY_ACTIONS)
    @axm09 Partition_HM_Table∈PARTITIONS→(SYSTEM_ERRORS⇸(ERROR_LEVEL_P×PARTITION_RECOVERY_ACTIONS⇸PROC_LEVEL_ERRORS))
end
```