
MODULE *epos4*

Possible *NMT* states

CONSTANT *NMT_Booting*, *NMT_PreOperational*, *NMT_Operational*, *NMT_Stopped*

$NMT \triangleq \{NMT_Booting, NMT_PreOperational, NMT_Operational, NMT_Stopped\}$

VARIABLES *nmt_state*, *nmt_requested*

$vars \triangleq \langle nmt_state, nmt_requested \rangle$

$TypeOK \triangleq \begin{array}{l} \wedge nmt_state \in NMT \\ \wedge nmt_requested \in NMT \end{array}$

Received a *BootUp* message

$NMT_BootUp \triangleq \begin{array}{l} \wedge nmt_state = NMT_Booting \\ \wedge nmt_state' = NMT_PreOperational \\ \wedge UNCHANGED\ nmt_requested \end{array}$

State transition confirmation

$NMT_Transition_Confirmed \triangleq \begin{array}{l} \wedge nmt_state \neq nmt_requested \\ \wedge nmt_state' = nmt_requested \\ \wedge UNCHANGED\ nmt_requested \end{array}$

Request state transitions

$NMT_EnterPreOperational \triangleq \begin{array}{l} \wedge \vee nmt_state = NMT_Operational \\ \vee nmt_state = NMT_Stopped \\ \wedge nmt_requested = nmt_state \\ \wedge nmt_requested' = NMT_PreOperational \\ \wedge UNCHANGED\ nmt_state \end{array}$

$NMT_ResetCommunication \triangleq \begin{array}{l} \wedge \vee nmt_state = NMT_Operational \\ \vee nmt_state = NMT_PreOperational \\ \vee nmt_state = NMT_Stopped \\ \wedge nmt_requested = nmt_state \\ \wedge nmt_requested' = NMT_Booting \\ \wedge UNCHANGED\ nmt_state \end{array}$

$NMT_ResetNode \triangleq \begin{array}{l} \wedge \vee nmt_state = NMT_Operational \\ \vee nmt_state = NMT_PreOperational \\ \vee nmt_state = NMT_Stopped \\ \wedge nmt_requested = nmt_state \end{array}$

$$\begin{aligned} & \wedge nmt_requested' = NMT_Bootng \\ & \wedge \text{UNCHANGED } nmt_state \end{aligned}$$

$$\begin{aligned} NMT_StartRemoteNode \triangleq & \wedge \vee nmt_state = NMT_PreOperational \\ & \vee nmt_state = NMT_Stopped \\ & \wedge nmt_requested = nmt_state \\ & \wedge nmt_requested' = NMT_Operational \\ & \wedge \text{UNCHANGED } nmt_state \end{aligned}$$

$$\begin{aligned} NMT_StopRemoteNode \triangleq & \wedge \vee nmt_state = NMT_Operational \\ & \vee nmt_state = NMT_PreOperational \\ & \wedge nmt_requested = nmt_state \\ & \wedge nmt_requested' = NMT_Stopped \\ & \wedge \text{UNCHANGED } nmt_state \end{aligned}$$

$$\begin{aligned} Init \triangleq & \wedge nmt_state = NMT_Bootng \\ & \wedge nmt_requested = NMT_PreOperational \end{aligned}$$

$$\begin{aligned} Next \triangleq & \vee NMT_BootUp \\ & \vee NMT_Transition_Confirmed \\ & \vee \vee NMT_EnterPreOperational \\ & \vee NMT_ResetCommunication \\ & \vee NMT_ResetNode \\ & \vee NMT_StartRemoteNode \\ & \vee NMT_StopRemoteNode \end{aligned}$$

$$\begin{aligned} Live \triangleq & \forall s \in NMT : \\ & (nmt_requested = s) \leadsto (nmt_state = s) \end{aligned}$$

$$Spec \triangleq Init \wedge \Box [Next]_{\langle vars \rangle} \wedge WF_{vars}(Next)$$

\ * Modification History
\ * Last modified *Mon Jan 13 20:42:49 CET 2020* by *martin*
\ * Created *Mon Jan 13 12:39:13 CET 2020* by *martin*