AN EVENT TREE/FAULT TREE/EMBEDDED MARKOV MODEL APPROACH FOR THE PSAM-8 BENCHMARK PROBLEM CONCERNING A PHASED MISSION SPACE PROPULSION SYSTEM

Diego Mandelli

The Ohio State University Nuclear Engineering
Program, Columbus ,OH, USA

Tunc Aldemir

The Ohio State University Nuclear Engineering
Program, Columbus ,OH, USA

Enrico Zio

Politecnico di Milano
Dipartimento di Ingegneria
Nucleare, Milano, Italy

ABSTRACT

The object of analysis of the proposed benchmark exercise is a system of ion propulsion for a science mission to the outer solar system. The propulsion system consists of a single propellant tank and 5 propulsion assemblies. The mission consists of 7 phases with different durations and requirements for the number of operational assemblies. The objective of the benchmark exercise is to determine the time dependent reliability of the propulsion system over the planned mission duration using the provided reliability data. Mission success implies success of all phases. The solution approach here undertaken uses fault-tree/event-trees (ET/FTs) for each functional mode (start up, shut down, operation and no-operation) to generate the transition probabilities of a discrete-time, inhomogeneous embedded Markov chain consisting of 11 states. Results of the study show that assembly failure during Start Up and the Shut Down functional modes of the propulsion system significantly contribute to mission failure.

Copyright © #### by ASME

ISYSTEM DESCRIPTION

The system under consideration is an ion propulsion engine for science exploration in the outer solar system. It consists of a single propellant tank and 5 assemblies connected to the tank by a series of lines (dashed lines) as presented in Fig. 1.

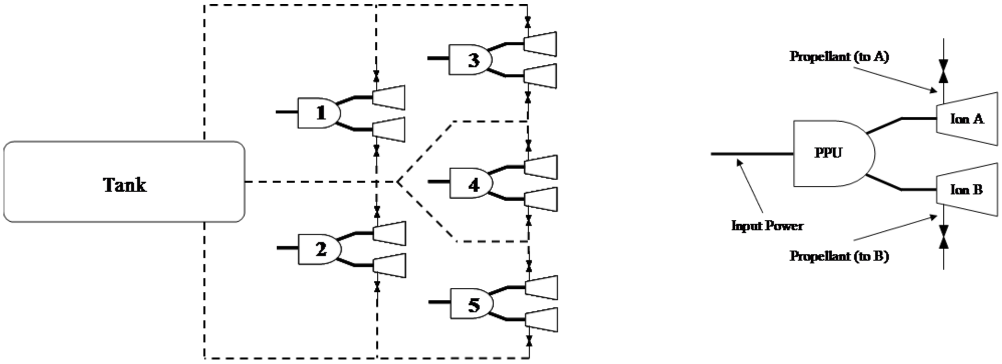

Figure 1. Propulsion system block diagram and assembly block diagram

Each assembly has 1 propulsion power unit (PPU), 1 main ion engine (Engine A), 1 ion engine (Engine B) in stand by redundancy, 1 propellant valve for each engine (V_A , V_B).

The mission consists of several phases and Fig. 2 shows phase durations, propulsion system operating time and the number of assemblies required for each phase along the Mission Elapsed Time (MET). All assemblies in each phase are in one of 4 operational modes: Start-Up (SU), Operation (OP), No-Operation (NO) and Shut Down (SD). Failure of an assembly causes it to be replaced by the lowest numbered standby assembly. The mission fails if the number of failed assemblies is greater or equal to 3. The mission also fails if leakages occur due to rupture of the propellant valves, tank or lines or failure to close of a valve after the shut down of the engine.

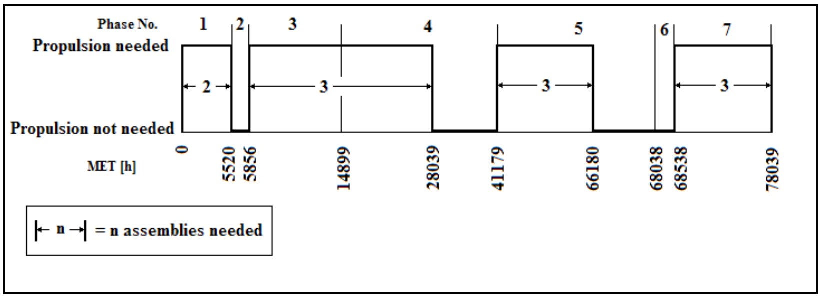

Figure 2. Mission profile temporal scheme as function of the Mission Elapsed Time (MET).

When an assembly is operating, the PPU provides power to just one ion engine. The other engine will be in a standby mode, unless failed. During Phase 1 the success criterion is propulsion from 2 assemblies. In all subsequent phases where the propulsion system is operating, the success criterion is propulsion from 3 assemblies. Relative to the assembly operation, the strategy is to use Assemblies 1 and 2 during the first phase. During subsequent phases, Assemblies 1 through 3 will furnish propulsion, if available. As mentioned above, failure of an assembly causes it to be replaced by the next lowest numbered standby assembly. Standby assemblies idle until they are needed to replace a failed assembly, and they are actuated in series (i.e., the lowest numbered assembly is first selected).

The strategy for the operation of an assembly is to begin with power from the PPU going to engine A. Engine A will continue to be the operating engine of the assembly until the engine fails. If Engine A fails, the PPU is first shutdown, switched to Engine B and re-started up to operate with engine B.

The objective of the benchmark exercise is to determine the time-dependent reliability of the propulsion system over the planned mission duration from the reliability data presented in Table 1.

Copyright © #### by ASME

Table 1. Reliability Data

Component	Failure Mode	Failure Probability or Rate	Effect
PPU	Fails to Start on demand	$1{\times}10^{-4}$ (per demand)	Assembly failure
	Fails to Operate	$1{\times}10^{-6}$ (per hour)	
	Fails to Shut Down	$1{\times}10^{-5}$ (per demand)	
	Fails to Switch to Engine B	$2{\times}10^{-6}$ (per demand)	
Ion Engine	Fails to Start on demand	$3{\times}10^{-5}$ (per demand)	Loss of Engine
	Fails to Operate	$2{\times}10^{-5}$ (per hour)	
	Fails to Shut Down	$3{\times}10^{-6}$ (per demand)	
Propellant Valve	Fails to Open on demand	$3{\times}10^{-4}$ (per demand)	Loss of Engine
	Fails to Close on demand	$3{\times}10^{-4}$ (per demand)	System failure
	External leakage	$5{\times}10^{-5}$ (per hour)	
Tank & Lines	External leakage	$1{\times}10^{-6}$ (per hour)	System failure

RELIABILITY MODEL

The approach proposed in this paper to the solution of the benchmark problem is based on a combination of the event-tree/fault-tree (ET/FT) approach [1-6] coupled with an inhomogeneous embedded Markov chain [7]. The temporal variable (MET) in Fig. 2 is divided into k = 0,..., 79039 (mission duration) time nodes each of which is associated with a time step (1 hour for OP and NOP, 0 hour for SU and SD), a functional mode and the number of assemblies needed for the functional mode. The embedded Markov model is described in terms of: a high level Markov chain (HLMC) and a low level Markov chain (LLMC) built inside each state of the HLMC.

The HLMC states consist of all the possible configurations of the propulsion system in terms of assemblies which are not in a failure mode and, thus, available to provide the propulsion. Fig. 2 shows the 11 states identified for the HLMC from the mission profile graphically represented in Fig. 3.

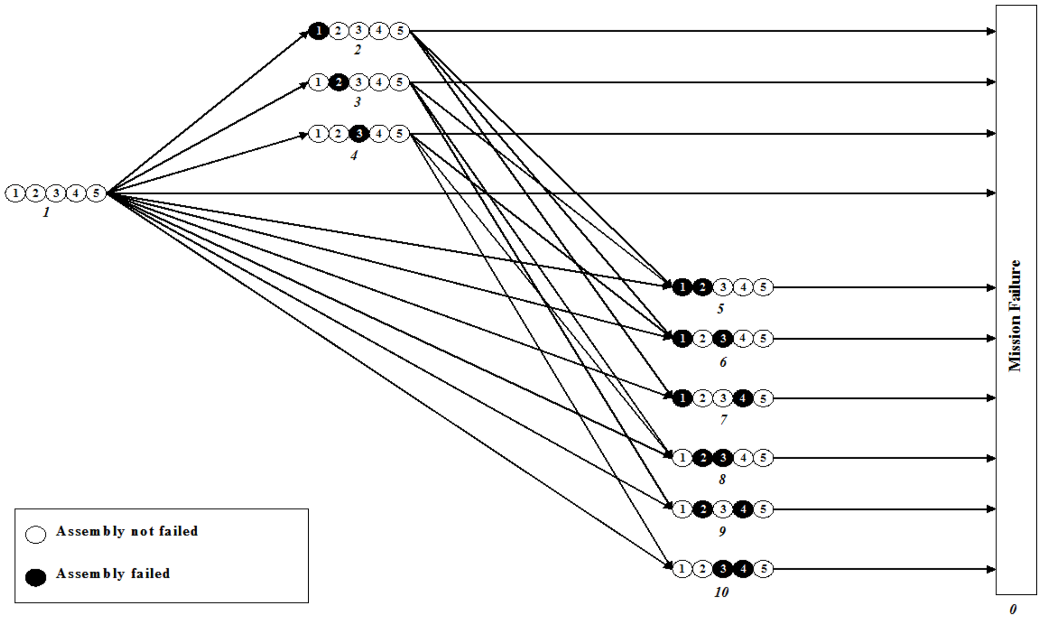

Figure 3. State definitions and possible transitions for the HLMC. Numbers in italics indicate states.

State 0 describes the failure of the mission and is regarded as an absorbing state. Fig. 3 also shows the possible transitions between system states. Transitions within states are possible but they are not shown in Fig. 3. From any state, the system transfers to State 0 if: a) the number of damaged assemblies is greater or equal to 3, b) leakages occur in the distribution lines or in the propellant tank, or, c) one or more propellant valves fail to close on demand.

Each assembly in each state of the HLMC is modeled through a LLMC as presented in Fig. 4.

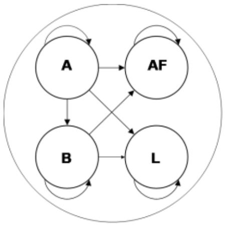

Figure 4. Low level Markov Chain.

Possible states for the LLMC are: i) propulsion is provided by engine A (State A), ii) propulsion is provided by engine B (State B), iii) assembly is in failure mode (State AF), d) leakages occur in the assembly during the closing phase of a valve (State L). The state probabilities $p_{k+1,m,n}(X)$ (with *X* = *A*, *B*, *AF* or *L*) of a LLMC for assembly *m* in state *n* state of the HLMC (see Fig. 4) at time node *k+1* are obtained from

$$\begin{aligned}
&p_{k+1,m,n}(A) = \pi_{k,m,n}(A|A)\bar{p}_{k,m,n}(A)\\
&p_{k+1,m,n}(B) = \pi_{k,m,n}(B|A)\bar{p}_{k,m,n}(A) + \pi_{k,m,n}(B|B)\bar{p}_{k,m,n}(B)\\
&p_{k+1,m,n}(AF) = \pi_{k,m,n}(AF|A)\bar{p}_{k,m,n}(A) + \pi_{k,m,n}(AF|B)p_{k,m,n}(B) + \bar{p}_{k,m,n}(AF)\\
&p_{k+1,m,n}(L) = \pi_{k,m,n}(L|A)\bar{p}_{k,m,n}(A) + \pi_{k,m,n}(L|B)\bar{p}_{k,m,n}(B) + \bar{p}_{k,m,n}(L)
\end{aligned} \tag{1}$$

$$(k = 0,1,2,;m = 1,\ldots,5;n = 0,\ldots,10)$$

where

- $\pi_{k,m,n}(X'|X)$ (*X, X'=A, B, AF* or *L*) is the transition probability from State *X* to *X'* of the LLMC for the assembly number *m* given that HLMC is at state *n* at the time node k-1 and HLMC is at state n of the at the time node k.
- $p_{k,m,n}(X)$(*X =A, B, AF* or *L*) is the probability for assembly *m* to be in State *X* of the LLMC given that HLMC is at state *n* of the at the time node *k-1*.
- $\bar{p}_{k,m,n}(X)$ (*X =A, B, AF* or *L*) is the probability for assembly *m* to be in State *X* of the LLMC given that HLMC is at state *n* of the at the time node *k*.

The quantities $\bar{p}_{k,m,n}(L)$in Eq.(1) provide the coupling between HLMC and LLMC. Later in this section it will be shown how they can be determined from the HLMC state and transition probabilities. Also, note that some transitions for the LLMC are impossible and subsequently the corresponding transition probabilities are zero in Eq.(1). For example, transition from state *B* to *A* cannot take place because an assembly can only be in state *B* if *A* has failed already. The transition probabilities $\pi_{k,m,n}(X'|X)$are determined using a classical ET/FT approach. Figures 5 through 7 show the ET/FTs corresponding to SU, OP and SD functional modes, respectively. For each assembly functional mode, transition probabilities for the LLMC are determined using values presented in Table 2 and Figs. 5, 6, 7. No ET/FT is presented for the NO mode since only leakages can occur from tanks, distribution lines and valves in this functional mode.

The overall procedure for the estimation of mission unreliability consists of the following steps:

1. Find functional mode for time node *k* from Fig. 2.
2. Find $\pi_{k,m,n}(X'|X)$in Eq.(1) from Table 2 and Figs. 5, 6 or 7 for the functional mode identified in Step 1 and for X, X'=*A, B, AF, L*.
3. Find $p_{k+1,m,n}(X)$(*X=A, B, AF* or *L*) from Eq.(1), using $p_{k,m,n}(X)$ and $\pi_{k,m,n}(X'|X)$determined from Step 2.
4. Find the probability $\Pi_k(n'|n)$(*n,n'*=1,…, 11) that the system goes from HLMC state *n* to state *n'* at time node *k* from the failure or the success of each of the five assemblies for the functional mode relevant to time node *k*. For example, for the transition $\Pi_k(2|1)$ we need the success of assemblies 2, 3, 4, 5 and the failure of the assembly number 1 (see Fig. 3) and subsequently

Copyright © #### by ASME

$$\Pi_k(2|1)=\left[\frac{\pi_{\mathrm{k,1,1}}(AF\,|\,A)p_{\mathrm{k,1,1}}(A)+\pi_{\mathrm{k,1,1}}(AF\,|\,B)p_{\mathrm{k,1,1}}(B)}{p_{\mathrm{k,1,1}}(A)+p_{\mathrm{k,1,1}}(B)}\right] \times\prod_{r=2}^{5}\left[\frac{\pi_{\mathrm{k,r,1}}(A|A)p_{\mathrm{k,r,1}}(A)+\pi_{\mathrm{k,r,1}}(B|A)p_{\mathrm{k,r,1}}(A)+\pi_{\mathrm{k,r,1}}(B|B)p_{\mathrm{k,r,1}}(B)}{p_{\mathrm{k,r,1}}(A)+p_{\mathrm{k,r,1}}(B)}\right] \tag{2}$$

Thus, each of the state transition probabilities of the HLMC is the product of five terms (corresponding to the number of assemblies of the propulsion system) which take into account the success (S) or the failure (F) of the assemblies according to Table 2 and Fig. 3. For the assembly *m* of the state *n* of the HLMC, probability of failure or success at time node *k* will be, respectively,

$$\begin{aligned} P^F_{k,m,n} &= \frac{\pi_{\mathrm{k,m,n}}(AF\,|\,A)p_{\mathrm{k,m,n}}(A)+\pi_{\mathrm{k,m,n}}(AF\,|\,B)p_{\mathrm{k,m,n}}(B)}{p_{\mathrm{k,m,n}}(A)+p_{\mathrm{k,m,n}}(B)} \\ P^S_{k,m,n} &= \frac{\pi_{\mathrm{k,m,n}}(A|A)p_{\mathrm{k,m,n}}(A)+\pi_{\mathrm{k,m,n}}(B|A)p_{\mathrm{k,m,n}}(A)+\pi_{\mathrm{k,m,n}}(B|B)p_{\mathrm{k,m,n}}(B)}{p_{\mathrm{k,m,n}}(A)+p_{\mathrm{k,m,n}}(B)} \end{aligned} \tag{3}$$

Table 2. Scheme for the general transition from state n’ to state n of the HLMC.

n' / n	1	2	3	4	5	6	7	8	9	10
	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
1	S S S S S	0	0	0	0	0	0	0	0	0
2	F S S S S	S S S S S	0	0	0	0	0	0	0	0
3	S F S S S	0	S S S S S	0	0	0	0	0	0	0
4	S S F S S	0	0	S S S S S	0	0	0	0	0	0
5	F F S S S	F F S S S	F F S S S	0	S S S S S	0	0	0	0	0
6	F S F S S	F S F S S	0	F S F S S	0	S S S S S	0	0	0	0
7	F S S F S	F S S F S	0	0	0	0	S S S S S	0	0	0
8	S F F S S	0	S F F S S	S F F S S	0	0	0	S S S S S	0	0
9	S F S F S	0	S F S F S	0	0	0	0	0	S S S S S	0
10	S S F F S	0	0	S S F F S	0	0	0	0	0	S S S S S

F	Failure
S	Success
0	Transition impossible

5. Determine the HLMC state probabilities $P_{k+1}(n')$ for each state *n’* (*n*’=0,,…,10) (see Fig. 2) using the transition probabilities $\Pi_k(n'|n)$ determined in Step 4 and all the state probabilities $P_k(n)$ of the HLMC determined in the previous time node k from

$$P_{k+1}(n')=\sum_{n=0}^{10}\Pi_k(n'|n)P_k(n) \tag{4}$$

6. Calculate $\bar{p}_{k+1,m,n}(X)$ (X = *A*, *B*, *AF*, *L*) in Eq.(3) from

$$\bar{p}_{k+1,m,n}(X)=\sum_{i=0}^{10}\frac{\Pi_k(n|i)P_k(i)}{\sum_{s=0}^{10}\Pi_k(n|s)P_k(s)}\,p_{k+1,m,i}(X) \tag{5}$$

The denominator in Eq. (5) represents the probability that the propulsion system (Fig.1) is in HLMC state *n* at time node *k+1*. Equation 5 is obtained by decomposing the probability that assembly *m* is in state *X* and the propulsion system is in HLMC State *n* at time node *k*+1 first in terms of: a) probability that assembly *m* is in state *X* given that the propulsion system is in HLMC state *n* at time node *k*+1, and, b) conditional probability that the propulsion system is in HLMC state *n* at time node *k*+1 given that the system is in HLMC state *i* at time node *k*.

Copyright © #### by ASME

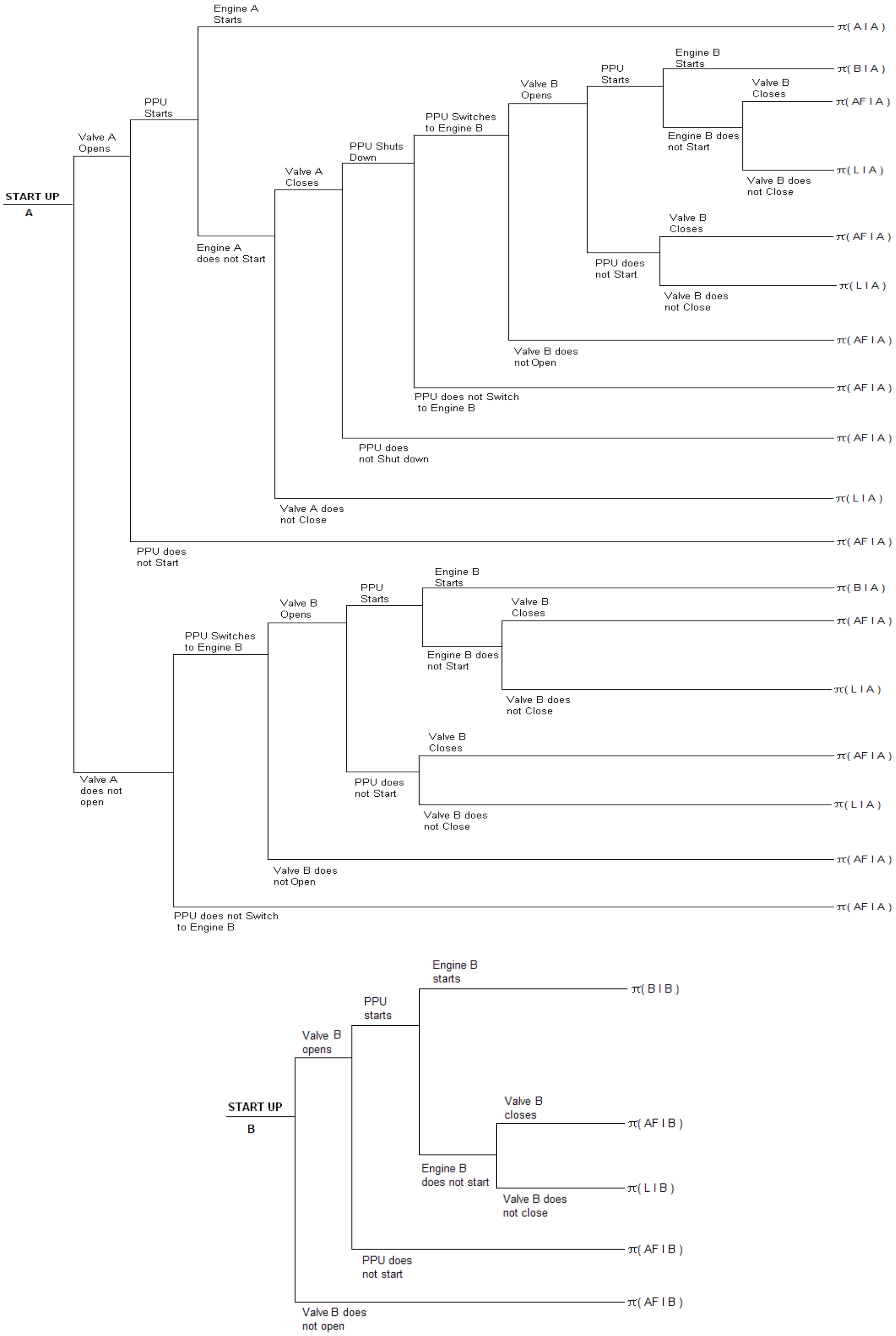

Figure 5. ET/FT for the SU mode.

Copyright © #### by ASME

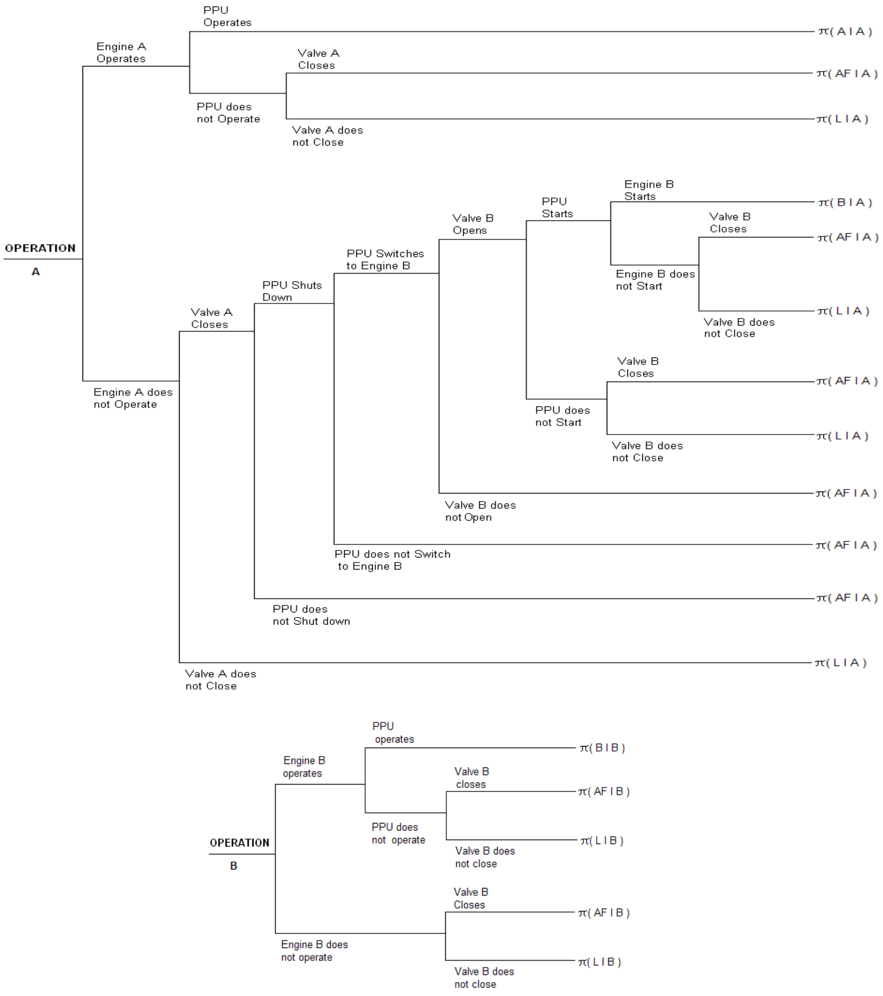

Figure 6. ET/FT for the OP mode.

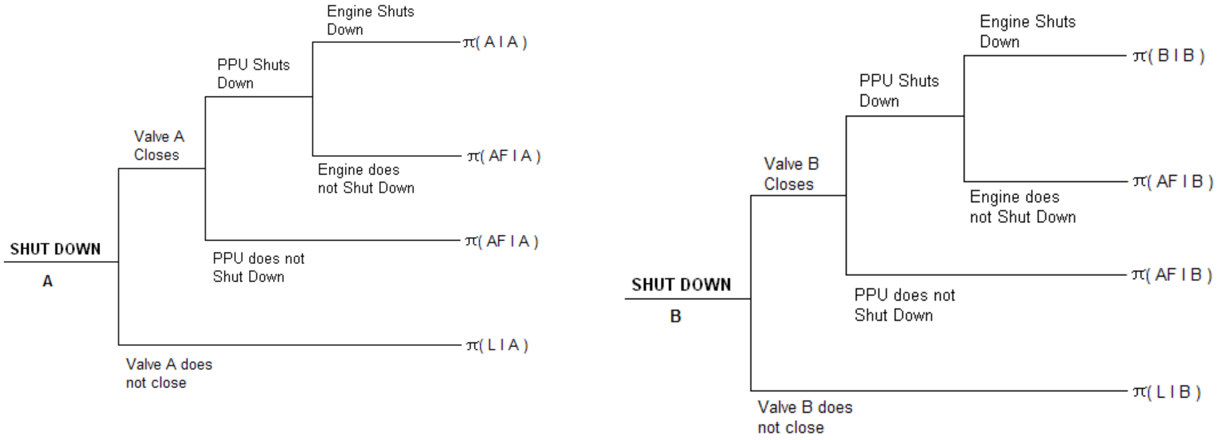

Figure 7. ET/FT for the SD mode.

Copyright © #### by ASME

COMMON CAUSE FAILURES

Common cause failures (CCF) have been modeled by taking the group conditional failure probabilities supplied in the benchmark problem specification (see Table 3) as β-factor values, i.e. the failure probability or rate p_t^i of component *i* (PPU, valve, engine) in each Figs. 5, 6 and 7 is determined from

$$p_t^i = (1+\beta)p_f^i \tag{6}$$

where p_f^i are as given in Table 1 and the β-factors are as given in Table 3.

Table 3. Common Cause Failure Modeling Values

Number of operational assemblies	β-factor [%]
2	8.0
3	4.0
4	2.0
5	1.0

MODEL IMPLEMENTATION AND RESULTS

The reliability model was implemented using the Java-Eclipse SDK platform. It is important to emphasize that the probability values for leakage event presented in the benchmark problem are high. The probability $R_\ell(t)$ that the mission fails due to leakage (except during SD mode) is :

$$F_\ell(t) = 1 - \exp\left(-\sum_{i=1}^{N} \lambda_i \cdot t\right)$$

where *N*=12 is the total number of components subject to leakage (10 valves, 1 tank and 1 distribution line) and the leakage failure rates, λ_i, are given in Table 1. Figure 8 shows that the probability that the system fails due only to leakage at the end of the mission (~80000 hours) is very close to 1.

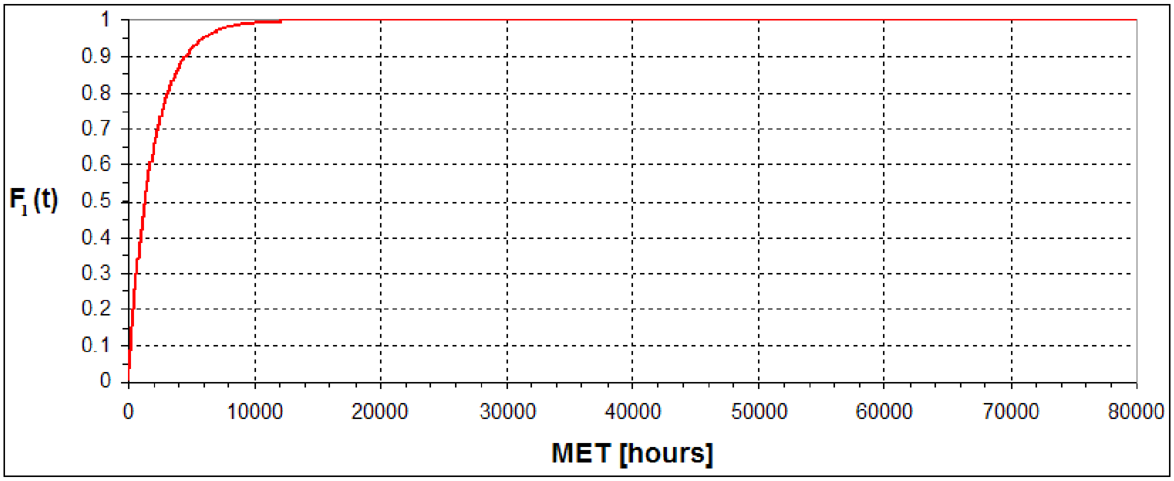

Figure 8. Mission Failure Probability as function of only leakage.

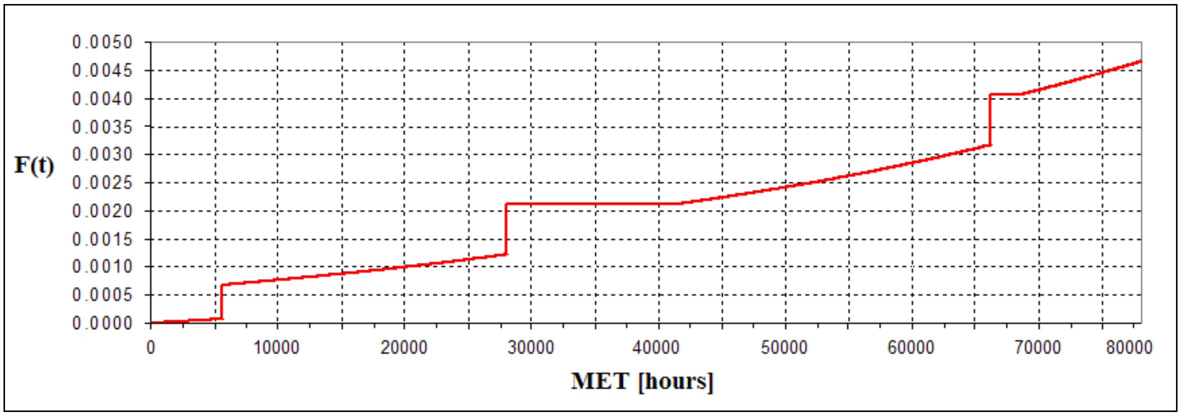

Figure 9. Mission Failure Probability of the entire propulsion system as a function of time.

Figure 9 shows the overall mission failure probability $F(t)$ (probability of HLMC State 0) due to all other effects. The mission failure probability (0.47%) is very low if leakage is not taken into account. This low values is attributed to both to the large number of assemblies used in the propulsion system over the maximum requested (5 vs. 3) and, not secondarily, to the stand-by engine present in each assembly (see Fig. 1). The steps in Fig.9 are attributed to system behavior during the SD functional mode and, more specifically due to the probability of failing to close of the propellant valve (see Table 1) when each assembly is shut down (see Fig. 7) while intervals which present relatively slower change in $F(t)$ are attributed to the NO functional mode where only leakage could occur (except during SD mode) but this event is not included in Fig.9. Note that the step changes occurs in correspondence of the times of charge in the mission phase as shown in Fig.2. Also, note that the likelihood of step changes originating from the SU modes is small, since Fig. 5 shows that at least two failure events need to occur for an assembly to fail (e.g. Engine A fails and Valve A does not close as shown in Fig.5) whereas only 1 failure event can lead to assembly failure during SD (e.g. Valve A does not close as shown in Fig.7).

CONCLUSION

This study introduces a new modeling formalism to determine the mission failure probability for the benchmark problem. An embedded Markov model is used in which the transition probabilities are determined from an appropriate ET-FT analysis. The possibility to implement complex control logic procedures with this formalism has been demonstrated, including the possibility to keep track of the history of each assembly. History dependence arises from the use of two engines in each assembly with different assembly startup procedures depending on the engine used. The formalism can account for this through coupling between LLMC and HLMC without the need to introduce auxiliary states.

The results of this study predict a very low mission failure probability for the benchmark problem if leakage of valves, tank and distribution lines are not taken into account.

REFERENCES

[1] WASH-1400, Reactor Safety Study, 1975.
[2] N.J. McCormick, Reliability and risk analysis, Academic Press, New York, 1981.
[3] PRA Procedures Guide, Vols. 1&2, NUREG/CR-2300, January 1983.
[4] E.J. Henley and H. Kumamoto, Probabilistic risk assessment, IEEE Press, NY, 1992.
[5] Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, NASA, 2002.
[6] Fault Tree Handbook with Aerospace Applications, NASA, 2002.
[7] M. Rausand and A. Hoyland, System Reliability Theory, Wiley, 2004.

Copyright © #### by ASME