

Reliability Analysis of a Dynamic Phased Mission System

Marc Bouissou
Electricité de France

and

Yves Dutuit
Université Bordeaux 1/LAP

With the increasing complexity and automation associated with systems encountered in the nuclear, aerospace, chemical, electronic, and other industries, phased mission analysis methodology is being recognized as the appropriate reliability analysis method for a large number of problems. A phased mission is a task, to be performed by a system, during the execution of which the system is altered such that the logic model changes at specified times. Thus, during a phased mission, time periods (phases) occur in which either the system configuration, system failure characteristics, or both, are distinct from those of any immediately succeeding phase. Phased mission techniques are required for proper analysis of problems when switching procedures are carried out or equipment is reassembled into new systems at predetermined times.

An important quantitative phased mission analysis problem is to calculate exactly or obtain bounds for mission unreliability, where mission unreliability is defined as the probability that the system fails to function successfully in at least one phase. Estimating the mission reliability by the product of the reliabilities of the phases usually results in an appreciable overprediction in system reliability, since basic events are shared among the logic models for the various phases” [1].

This paper aims to illustrate the use of two reliability analysis methods applied to a simple, but not trivial, problem. The system proposed as a test-case is due to J. B. Dugan [2] and enables us to compare the respective benefits and drawbacks of a Petri net-based approach [3,4] and of the so-called BDMP approach, recently published [5].

The system to be studied is a hypothetical example of dynamic phased system which consists of two main non-repairable components A and B, a non-repairable back-up component C, and nine switches that are used in different configurations over two consecutive phases as described hereafter:

Phase 1

- Phase one mission time is exponentially distributed with a mean value T_1 equal to 2,000 hours.
- Switches K_1 , K_2 , K_3 , K_4 , K_6 , and K_8 are normally closed.
- Switches K_5 , K_7 and K_9 are normally opened.
- Components A and B work in parallel and then they can fail ($\lambda_A = \lambda_B = 1.10^{-4} \text{ h}^{-1}$).
- Component C is a cold-spare for components A and B in phase one, and is activated automatically when the first failure occurs in either one of components A or B. For that to occur, some switches must be opened and some others must be closed with, at each time, a probability of failure on demand equal to 5.10^{-2} .

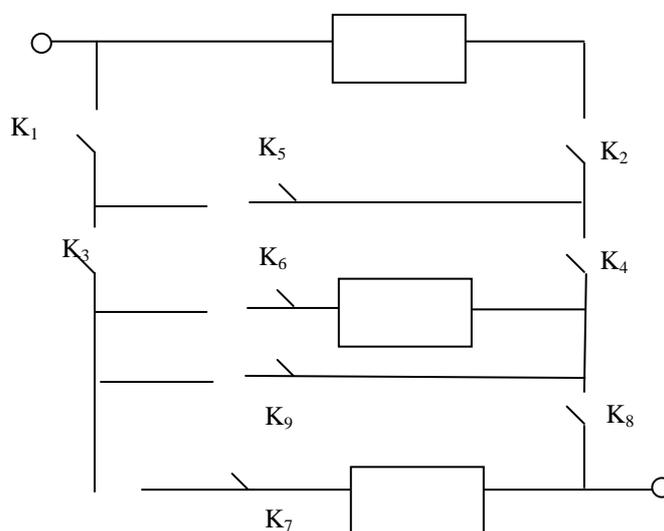
Component C can fail after it started ($\lambda_C = 1.10^{-4} \cdot \text{h}^{-1}$).

Phase 2

- Phase two mission time is exponentially distributed with a mean value T_2 equal to 1,000 hours.
- The positions of some switches are changed to enable the two active components to work in series. If component C has not been solicited during phase one, it can be used as a back-up during the second phase.

The system to be studied is shown in figure1.

Note that all components A, B and C must be passed through from left to right. Note also each time to failure of A, B and C is exponentially distributed and each failed component can be considered as a shunted component.



Expected results:

The twofold objective of this study is to compute the system reliability over the whole mission time $T_1 + T_2$, by using respectively PN and BDMP approaches and to compare their ability to model and assess system performance.

References

- [1] G.R. Burdick, J. B. Fussell, D. M. Rasmusson, J. R. Wilson, "Phased Mission Analysis. A Review of New Developments and An Application", *IEEE Trans. Rel.*, 26 : 1 (1977), pp. 43-49.
- [2] J. B Dugan, M. Zhu, K. J. Sullivan, "A Functional Test Suite for Quantitative Fault Tree Reliability Analysis", *Personal communication*.
- [3] Y. Dutuit, E. Châtelet, P. Thomas, J. P. Signoret, "Dependability Modelling and Evaluation by Using Stochastic Petri Nets : Application to Two Test-Cases", *Reliability Engineering and System Safety*, 55 : 2 (1997), pp.117 – 124.
- [4] D. C. Ionescu, E. Zio, A. C. Contantinescu, "Availability Analysis of a Safety System of a Nuclear Reactor", *Proceedings of KONBIN'03 Conference*, vol. 2, pp. 225 – 233.
- [5] M. Bouissou, J. L. Bon, "A new formalism that combines advantages of fault trees and Markov models : Boolean logic driven Markov processes", *Reliability Engineering and System Safety*, 82 : 2 (2003), pp. 149 – 164.