

Reliability Control of Fault Tolerance Units

Vladimir Rykov

Dept. of Appl. Math. and Comp. Modeling
Russian State University of Oil&Gas
Leninskiy prosp., 65, 117917 Moscow
Russia
rykov@rykov1.ins.ru

Dmitry Efrosinin

Dept. Theory of Prob. und Stat.
Russian Peoples' Friendship University
Johannes Kepler University
Russia, Austria
Dmitry.Efrosinin@jku.at

Abstract

Reliability control model for fault tolerance units under different repair policies with respect to cost minimization and/or availability maximization criteria are proposed. Optimization algorithms and appropriate computer routines are given. Some numerical examples for the approach illustration are considered.

1 Introduction and Motivation

Many of up-to-date complex technical systems are characterized by implemented system of the state control. Presence of the implemented system of control (SoC) leads to the fact that the system becomes a so-called Fault Tolerance System. In the paper we limit ourselves by the studying of non-separable controllable Fault Tolerance Unit (FTU).

Let us consider the reliability model of some single FTU. Beginning from normal functioning (NF) state a FTU typically passes through the several stages: error detection (ED), damage assessment and confinement (DA), error recovery (ER), and fault treatment (FT) before it falls into the failure state. Nevertheless, due to unexpected failure it also could fails from any intermediate state (see Figure 1).

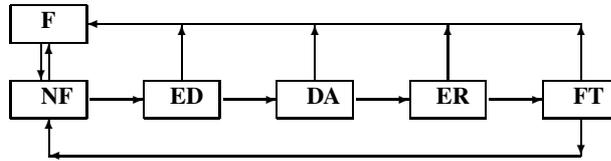


Figure 1: State transition scheme for Single FTU Model.

The SoC detects the faults and correct them itself or give a signal about a necessity of the repair. Some delays and costs (or rewards loss) are needed for the repair. In case if the unit is turned for the repair the further degradation impossible and it is supposed that after repair it becomes "as good as new" one. Different kind of preventive maintenance was considered by many authors (see Gertsbakh (1) and the references therein).

Thus, we deal with the model of a preventive maintenance system based on a state control and the problem consists in a choice of maintenance policy to optimize the given criterion. The different types of criteria could be considered: reward maximization, cost minimization or availability maximization, etc.

2 A Problem Statement

Consider a model of reliability control of some single FTU. The unit could be in different fault stages (gradual failures), it begins to operate from a normal functioning state, and during its operation it transfers from one fault stage to another, and these stages are under control. It means that a gradual failure can be detected and repaired. After any repair the unit is returned back to its initial state.

The SoC is usually much more reliable. Nevertheless, this system also can fail, and it leads to fail the possibility to observe the real system state. We will consider several different cases of reliability and observability of the SoC:

- (i) SoC is absolutely reliable;
- (ii) SoC is non-reliable but its states are observable;

(iii) SoC is non-reliable and its states are non-observable.

Let us label the fault stage by integers and suppose for the generality any, say m , number of stage. We will also mark the state of SoC by integer i , where $i=0$ means that the SoC is in a "good" condition, and $i = 1$ means that the SoC fails. We will denote the state space by E with the failure state F . So, in general case we will consider the system with two dimensional system space of states $E = \{(i, j) : i = 0, 1; j = 0, 1, \dots, m, F\}$. This state space is different under different assumptions, and its strong definitions will be introduced in appropriate sections.

In this paper we limited ourselves with the Markov models. Denote the process describing the FTU behavior by $X = \{X(t), t \geq 0\}$.

Suppose also that the repair in intermediate fault stage k is assumed to involve a fixed additional cost c_k , while the repair after the full unit failure (in state F) does cause expenses c_F . For the considered cost structure the loss functional can be written in the form

$$G(t) = \int_0^t \left(\sum_{0 \leq i \leq k-1} c_i 1_{\{X(u)=(1,i)\}} + c_k 1_{\{X(u)=(0,k)\}} + c_F 1_{\{X(u) \in F\}} \right) du \quad (1)$$

The system control should be described in terms of admissible strategies $\delta \in \Delta$. Jointly with the process behavior description and given initial state x these strategies generate the probability measure \mathbf{P}_x^δ on the trajectories space of the process with an appropriate expectation \mathbf{E}_x^δ (see (2)).

The problem of the reliability control consists in a construction of the strategy that minimizes the long run average cost

$$g(\delta) = \lim_{t \rightarrow \infty} t^{-1} \mathbf{E}_x^\delta G(t) \implies \min \quad (2)$$

over all admissible strategies $\delta \in \Delta$.

3 Description of the Results

As we have mentioned above we consider three models with different reliability and observability of the SoC and compare the efficiency of a control with non-controllable reliability FTU.

FTU with Non-Controllable Reliability

Suppose that the transition time from i -th to $(i + 1)$ -st gradual stage and non-controllable (immediate) failure at this stage have exponential distributions with parameters λ_i and ν_i , respectively, and the repair time exponentially distributed with parameter μ_F . Then the behavior of the FTU could be represented by a Markov process $X = \{X(t) : t \geq 0\}$ with a discrete state space $E = \{0, 1, \dots, m, F\}$ and corresponding transition intensities.

FTU with Absolutely Reliable SoC

For the model with *controllable* reliability the gradual fault stages are under control. It means that a gradual faults can be detected and repaired. After any repair the unit is returned back to its initial state. In any gradual fault stage some decision about repair should be taken. We will suppose that the repair time from the state i has an exponential distribution with parameter μ_i . Under the same assumption the behavior of the unit now is represented by a *controllable* Markov process $X = \{X(t) : t \geq 0\}$ with the same state space $E = \{0, 1, \dots, m, F\}$ and a decision space $A = \{0, 1\}$, where decision $d = 0$ means "do not begin repair", while decision $d = 1$ means "begin repair".

It is reasonable to suppose that the optimal policy possesses the threshold property, i.e. one needs only to find the state k for the maintenance beginning.

FTU with Non-Reliable and Observable SoC

For the system with non-reliable and observable SoC it is reasonable immediately begin the maintenance if the SoC fails because in this case the unit becomes non-controllable. Under the same assumptions as before to model the FTU behavior in case of non-reliable SoC we have to consider a two dimensional state space $E = \{(i, j) : i = 0, 1; j = 0, 1, \dots, m, F\}$, where the first component denotes the state of the SoC: $i = 0$ means the SoC is in a "good" condition, and $i = 1$ means that the SoC fails (with intensity γ_i), and j describes the states of FTU as in previous case. Thus for the control policy f_k – "send the unit for repair at the state k ", the unit behavior could be described by

a two-dimensional Markov process $X = \{X(t) : t \geq 0\}$ with the discrete state space E and corresponding transition intensities.

FTU with Non-Reliable and Non-Observable SoC

For investigation of the system with non-reliable and non-observable SoC we will use the same Markov process $\{X(t) : t \geq 0\}$ with state space $E = \{(i, j) : i = 0, 1; j = 0, 1, \dots, m, F\}$ as for the previous model. In this case, however, the failure of the SoC (states with first component equals to 1) does not observable, and the application of the Markov decision theory becomes enough complicated. The problem will be simplified if we limit ourselves by the threshold policies f_k only. In this case, because the failure of the SoC is not observable, the behavior of the process in the states $(1, j)$ is exactly the same as in $(0, j)$ with only possibility to go to the exhaustive state $(1, m)$ through the states with non-observable failed SoC.

For each models we obtain the steady state probabilities for corresponding Markov process $\pi_i, i = 0, 1, \dots, m$ and the total failure probability π_F . With respect to the cost minimization criterion we consider the functional $g_k, k = 1, 2, \dots, m$, where

$$g_k = c_F \pi_F, \quad \text{for FTU with Non-Controllable Reliability;}$$

$$g_k = c_k \pi_k + c_F \pi_F, \quad \text{for FTU with Absolutely Reliable SoC;}$$

$$g_k = \sum_{0 \leq i \leq k-1} c_i \pi_{1i} + c_k \pi_{0k} + c_F \pi_F, \quad \text{for FTU with Non-Reliable and Observable SoC;}$$

$$g_k = c_k \pi_k + c_F \pi_F, \quad \text{for FTU with Non-Reliable and Non-Observable SoC.}$$

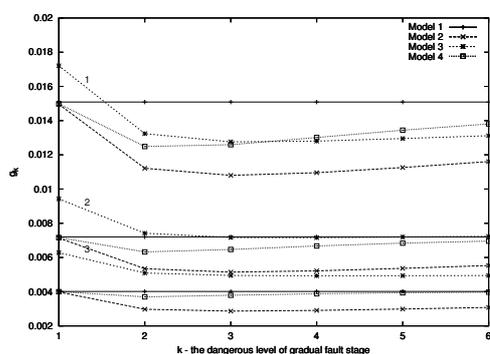
In case of the availability $a_k = 1 - (\pi_k + \pi_F)$ maximization one should put $c_F = c_i = 1$ for all $i = 1, \dots, m$, and minimize the same functional. For minimization of the full failure probability π_F one has to accept $c_F = 1, c_i = 0, (i = 1, \dots, m)$.

4 Examples

The optimization problem consists in calculation of the appropriate function g_k for $k = 1, \dots, m$, where $m = 6$ fault stages were considered. All the intensities and costs will be normalized in such a way that $\mu_F = 1$ and $c_F = 1$ and the entire failure intensities for different models coincide.

The results of the long-run average loss calculation for different models when the values of initial system parameters are varied are summarized in the diagrams shown in Figures 2–4 bellow. The graph represents values g_k as a function of different possible dangerous level k to begin the maintenance and repair.

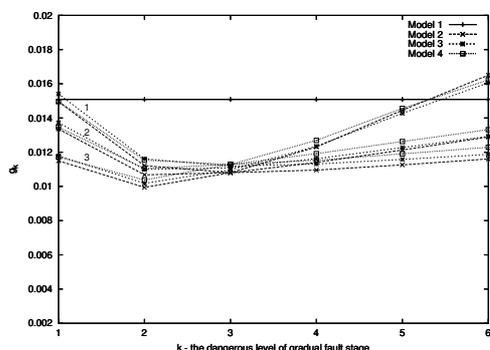
In Figure 2 it is shown the function g_k when the failure intensities, λ_i and ν_i increase. The controllable reliability model is the best with optimal solution $k_{opt} = 3$. But the model with non-reliable SoC and non-observable states ($k_{opt} = 2$) is better as the same model with observable states ($k_{opt} = 3$). In these examples all repair costs $c_i = 1$, therefore the function $a_k = 1 - g_k$ represents the availability.



i	0	1	2	3	4	5	6
(1) λ_i	0.027	0.054	0.134	0.268	0.456	0.698	-
(2) λ_i	0.013	0.025	0.064	0.127	0.216	0.331	-
(3) λ_i	0.007	0.014	0.035	0.071	0.120	0.184	-
(1) ν_i	0.003	0.005	0.013	0.027	0.046	0.070	0.099
(2) ν_i	0.001	0.003	0.006	0.013	0.022	0.033	0.047
(3) ν_i	0.001	0.001	0.004	0.007	0.012	0.018	0.026
μ_i	2.149	2.147	2.145	2.143	2.141	2.139	2.136
γ_i	0.005	0.010	0.025	0.050	0.085	0.13	-
c_i	1.000	1.000	1.000	1.000	1.000	1.000	1.000

Figure 2: The long-run average loss g_k under the variation of the failure intensities, λ_i and ν_i .

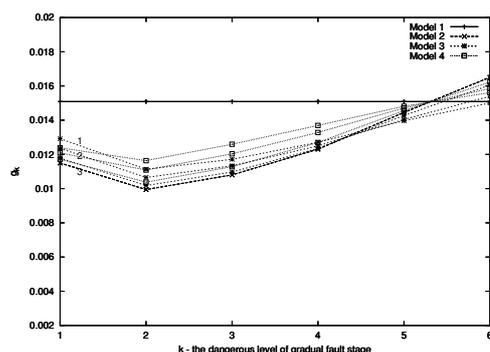
Figure 3 represents the function g_k under the variation of the repair intensities μ_i . In this figure the total repair intensity remains the same for all the models.



i	0	1	2	3	4	5	6
λ_i	0.027	0.054	0.134	0.268	0.456	0.698	-
ν_i	0.003	0.005	0.013	0.027	0.046	0.070	0.099
(1) μ_i	2.149	2.147	2.145	2.143	2.141	2.139	2.136
(2) μ_i	2.637	2.473	2.308	2.143	1.978	1.813	1.648
(3) μ_i	3.429	3.000	2.571	2.143	1.714	1.286	1.000
γ_i	0.001	0.002	0.005	0.010	0.017	0.026	-
c_i	1.000	1.000	1.000	1.000	1.000	1.000	1.000

Figure 3: The long-run average loss g_k under the variation of the repair intensities μ_i

The influence of the SoC failure intensities γ_i is investigated in Figure 4. For the large values of γ_i the non-observable case of the model with non-reliable SoC is better than the observable case.



i	0	1	2	3	4	5	6
λ_i	0.027	0.054	0.134	0.268	0.456	0.698	-
ν_i	0.003	0.005	0.013	0.027	0.046	0.070	0.099
μ_i	3.429	3.000	2.571	2.143	1.714	1.286	0.857
(1) γ_i	0.005	0.010	0.025	0.050	0.085	0.130	-
(2) γ_i	0.003	0.006	0.015	0.030	0.051	0.078	-
(3) γ_i	0.001	0.002	0.005	0.010	0.017	0.026	-
c_i	1.000	1.000	1.000	1.000	1.000	1.000	1.000

Figure 4: The long-run average loss g_k under the variation of the SoC failure intensities γ_i

5 Conclusion

The Markov models of the controllable reliability of fault tolerance units under different assumptions about system of control reliability are considered. In the paper we demonstrate the analytic expressions for the steady state probabilities and loss functional. Algorithm and some numerical examples are included. The results show that for the large set of the values for initial system parameters the models with SoC are better than non-controllable model. The quality of different models with SoC, e.g. in sense of different values of the long-run average loss, may vary when the values of system parameters change.

References

- [1] Gertsbakh I. (2000) *Reliability theory with application to preventive maintenance*. Springer-Verlag.
- [2] Kitaev M., Rykov V. (1995) *Controlled Queueing Systems*. CRC Press. Boca Raton.
- [3] Dimitrov B., Rykov V., Stanchev P. (2002) On Multi-State Reliability Systems. In: *Proceedings MMR-2002*. Trondheim (Norway) June 17-21, 2002.
- [4] Serfozo R. (1999) *Introduction to Stochastic Networks*. Springer-Verlag. N.-Y., 300p. (ISBN 0-387-98773-8)