DESIGN TESTABILITY ANALYSIS OF AVIONIC SYSTEMS

Igori B. Spiridonov
•
IRKUT Corporation, Moscow, 125315, Russia
Igori.Spiridonov@irkut.com

Armen S. Stepanyants, Valentina S. Victorova
•
Institute of Control Sciences (IPU RAN), Moscow, 117997, Russia
lfvrk@ipu.ru, ray@ipu.ru

ABSTRACT

This paper summarizes the result of an effort to develop a unified approach to design-driven testability evaluation of avionic systems. These systems include both internal diagnostic equipment referred to as built-in-test (BIT) and external off-line test equipment. At the designing stage an adequate database to evaluate the quality of the BIT is the failure mode and effect analysis. In the paper various mathematical indices are suggested and constructed to quantify testability of avionic systems. The indices provide the needed flexibility for representing structural and reliability properties of the controlled system. Analytical model for evaluation BIT performance impact on the system's reliability is discussed.

1 BIT PERFORMANCE IMPACT ON SYSTEM RELIABILITY

Evaluation of the technical condition of the avionic systems is ensured by the presence of built-in diagnostic functions and monitoring tools – BIT. BIT performance defines testability of the systems or its adaptation to detect and isolate failures to the replaceable assembly level. Operational integrated BIT monitoring of system's components provides effective usage of spares, reconfiguration and graceful degradation, ensuring thereby the fault-tolerance and safety of avionic system. However, the BIT is not ideal – first, it can refuse to act, and, secondly, not all failures and events can be recognized by BIT. Therefore, in order to ensure high levels of reliability and safety of avionic systems it is required to conduct a thorough reliability analysis, taking into account many factors, one of which is characteristics of BIT (Victorova et al. (2007), Victorova&Stepanyants (2008)).

So, the role of diagnostic systems should be judged by the impact of their characteristics on the probability indices of reliability and safety. We will study the reliability of a recoverable system comprising two identical sub-systems that are parallel in terms of reliability. We assume absolute BIT reliability but not absolute fault coverage. BIT can identify only part of sub-system failures and recovery is possible only after failure detection by BIT. Under this assumption the parallel system can be represented by controlled/recoverable and uncontrolled/unrecoverable series parts as shown in Figure 1. The percentage of all sub-system faults or failures that BIT can detect is denoted as η. We make assumption about exponential failure and repair distribution with parameters λ and μ respectively. Then failure rates of controlled part of the sub-system and uncontrolled part are equal $\eta\lambda$ and $(1-\eta)\lambda$ respectively.

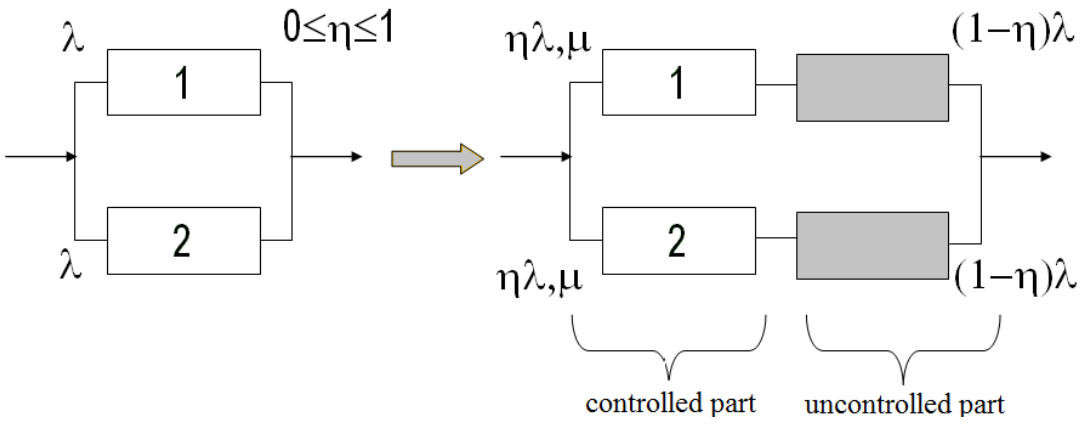

Figure 1. Duplicate repairable system with partial BIT

Let us consider the special treatment of system recovery when repairable actions start only after mission termination. This mode is typical for avionic systems when restoration is carried out only on the ground. Markov reliability model for this case is shown in Figure 2.

To determine the transition rate from state 2 to state 5 it is necessary to calculate conditional mean time to subsystem failure provided that the failure occurred during mission time interval $(0,t_m)$ $T_{av/tm}$:

$$T_{av/t_m} = M\{T/T<t_m\} = \int_0^{t_m} tf(t/t<t_m)dt = \int_0^{t_m} td\frac{F(t)}{F(t_m)} = \frac{1/\lambda - e^{-\lambda t_m}(t_m + 1/\lambda)}{1-e^{-\lambda t_m}}, \qquad (1)$$

where F(t) and f(t) are distribution function and distribution dencity of stochastic time to failure T. Derivation of Eq.(1) was done in Gnedenko et al.(1969).

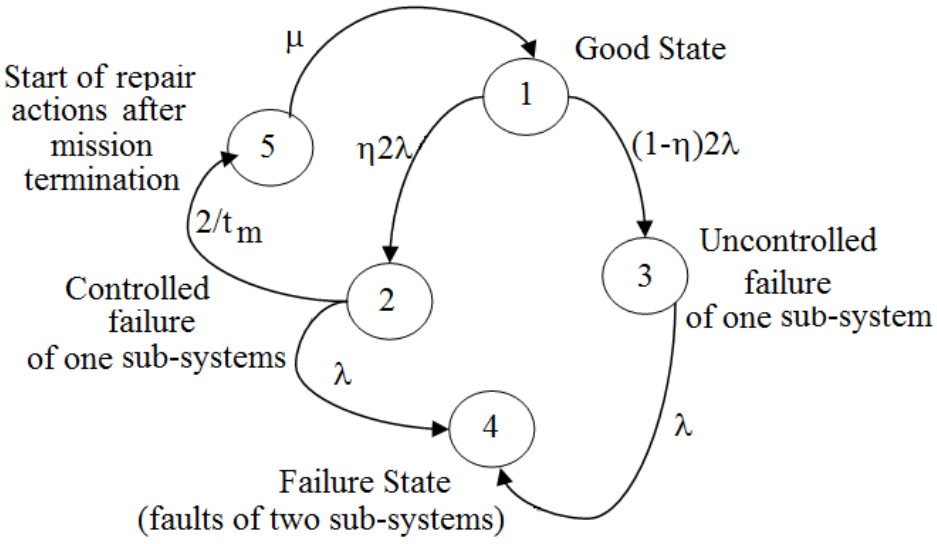

Figure 2. Markov reliability model

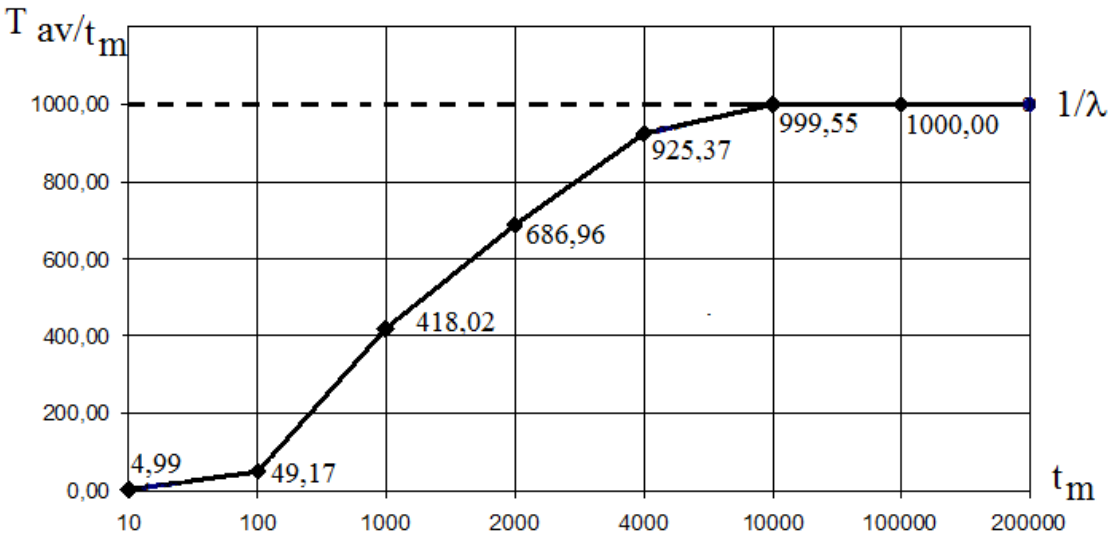

Figure 3. Conditional mean time to failure curve

If $t_m << 1/\lambda$ then $T_{av/tm} \approx t_m/2$. If $t_m > 1/\lambda$ then $T_{av/tm} \to 1/\lambda$. Chart in Figure 3 confirms these relations. Therefore, for avionic systems, which mission (flight) time is not more than a few hours, one can assume that the failure of subsystem occurs in the middle of the flight interval, and hence the transition rate from state 2 to state 5 is equal to $2/t_m$.

Reliability markov model of the duplicate repairable system with partial BIT was calculated at time interval (t = 0÷8760 hours). Probability of the system failure Q (probability of state 4) was calculated varying percent detection from 0 to 1. Normed $Q(\eta)$ curve from Figure 4 shows that even 50% failure detection reduces the probability of the system failure in hundreds of times. When η is close to 100% failure probability is reduced in more than thousand of times.

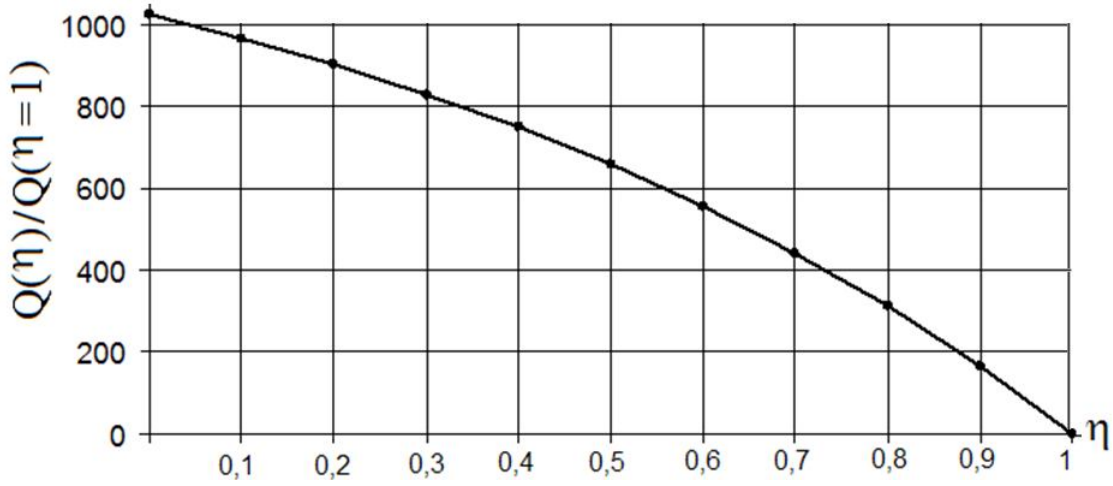

Figure 4. Normed curve of the system failure probability

2 TESTABILITY MODELS AND INDICES

The main characteristics of BIT equipment are percent detection and percent isolation.

2.1 Percent Detection Definition

Percent detection describes completeness of system's monitoring by BIT. In general, the quality of BIT is determined by the list of elements (modules), which failures are detected. Therefore, percent detection could be defined by the ratio of the number of controlled items to the total number of items in the system. However, for the joint reliability&testability modeling we should include some probabilistic constituent in percent detection definition. The usefulness of such approach consists in splitting the total failure flow into two components – the failures detected by the BIT and latent failures. Percent detection in this case can be defined as the conditional probability of failure detection, provided that the failure occurred:

$$\eta=\text{Prob}\{\text{failure is detected/failure occurred}\} = \frac{1-e^{-\int_0^t \Lambda_c(\tau)d\tau}}{1-e^{-\int_0^t \Lambda(\tau)d\tau}}, \quad (2)$$

where Λ - total failure rate of the system, Λ_c – total failure rate of detected by BIT failures.

After averaging the failure rates on the interval (0, t), we have

$$\eta = \frac{1-e^{-\Lambda_{cav}t}}{1-e^{-\Lambda_{av}t}}, \quad (3)$$

where $\Lambda_{av} = \frac{1}{t}\int_0^t \Lambda(\tau)d\tau, \quad \Lambda_{av}t << 1.$

Common percent detection Eqs. (2,3) in the case of exponential distribution is most useful to set as a ratio of the total failure rates of controlled components to total failure rates of all system components, i.e.

$$\eta = \frac{\sum_{j\in K}\lambda_j}{\sum_{i=1}^{n}\lambda_i}, \quad (4)$$

where n is the total number of elements of the system; K-subset of the controlled components; λ_i is failure rate of the i^{th} component. In this case percent detection is defined as stationary conditional probability of failure detection, provided that the failure occurred.

2.2 Percent Isolation Definition

Percent isolation characterizes BIT resolving ability. Percent isolation is diverse feature. For example, you can understand the percent isolation as the resolution of fault location in the hierarchy of the failed system components: subsystem, assembly, part. In this paper percent isolation will be determined through LRUs - Line Replaceable Unit as follows. If, in the event of a failure, the BIT points to a subset of elements that might be failed, then these items simultaneously removed (may be including not failed items) and replaced with a good LRUs (this is the specific of maintenance services). Similar to the detection isolation can be defined as percent of faults or failures that BIT system will isolate to a specified level (for example, to 1 LRU, 2 LRU, 3 LRU…). Therefore,

percent isolation can be represented by a discrete distribution. Stationary probabilities γ_k of this distribution are calculated as

$$\gamma_k = \frac{\sum_{j \in G_k} \lambda_j}{\sum_{i=1}^{n} \lambda_i}, \quad (5)$$

where G_k – subset of detected fault or failures results in removal of k LRUs.

Another stochastic characteristic of percent isolation γ may be suggested as ratio of mathematical expectation of numbers of detected failures ($n_f(t)$) to mathematical expectation of number of component removals ($n_r(t)$) for a specified time interval (0÷t):

$$\gamma = \frac{M\{n_f(t)\}}{M\{n_r(t)\}} \quad (6)$$

The advantage of the last definition is that percent isolation, calculated according to Eq. (6), may be associated with known logistics measure MTBUR (mean time between unscheduled removals). MTBUR is calculated as $t/M\{n_r(t)\}$.

2.3 Complex Measure of BIT Quality

In this section we will present complex performance measure of BIT, taking into account both considered detection and isolation characteristics and two modes of BIT possible failures.

Let us denote the following stochastic events:

A – good state of the controlled system

$\overline{A}$ - failure state of the controlled system

B - BIT indicates controlled system state as good state

$\overline{B}$ - BIT indicates failure of controlled system

Then we can formally define the following results of interaction between the system and BIT:

$A \wedge B$ - the system is good and BIT indicates good state of the system

$A \wedge \overline{B}$ - the system is good, but BIT indicates fault of the good system. This type of BIT failure is known as false alarm.

$\overline{A} \wedge B$ - the system is in failure state, but BIT does not detect fault and indicates good state of the system.

$\overline{A} \wedge \overline{B}$ - the system is in failure state and BIT detects fault and indicates failure state of the system.

Let us define quality measure, named BIT certainty or integrity, as the sum of the probabilities of events $A \wedge B$ and $\overline{A} \wedge \overline{B}$:

$$D = P(A \wedge B) + P(\overline{A} \wedge \overline{B}) \quad (7)$$

Then BIT uncertainty $\overline{D}$ is

$$D = P(A \wedge \overline{B}) + P(\overline{A} \wedge B) \quad (8)$$

Detailed expressions of the terms of BIT uncertainty Eq. (8) are

$$P(A \wedge \overline{B}) = P(A)P(\overline{B}/A), \; P(\overline{A} \wedge B) = P(\overline{A})P(B/\overline{A}) \quad (9)$$

Where $P(A)$ – probability of good state of controlled system, $P(\overline{A})$ – probability of failure state of controlled system, $P(\overline{B}/A)$ conditional probability of BIT failure indication on condition that system is good, $P(B/\overline{A})$ conditional probability of BIT indication good system state on condition that system is in failed state.

To calculate these conditional probabilities we will use event tree model (Kumamoto&Henley (2000)) and will take into account BIT percent detection, false alarms and "nonoperate" BIT's failure mode (detailed description of this approach is presented in Victorova (2009)).

We denote possible BIT events as

C – BIT is in good state

$\overline{C}_{no}$ – BIT is in failure state and failure mode is "nonoperate"

$\overline{C}_{fa}$ – BIT is in failure state and failure mode is "false alarm"

Figure 5 presents event tree for calculation the conditional probability of BIT failure indication under good system $P(\overline{B}/A)$.

Figure 6 presents event tree for calculation the conditional probability of BIT indication good system state on condition that system is in failed state $P(B/\overline{A})$.

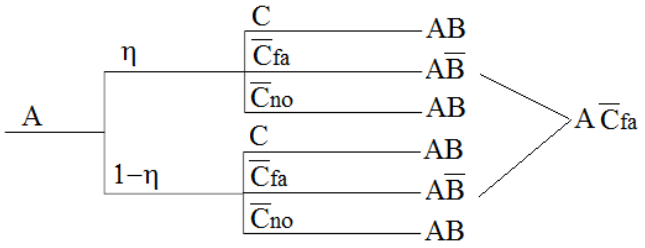

Figure 5. Event tree model for calculation $P(\overline{B}/A)$

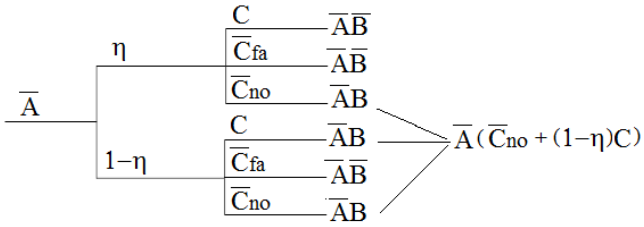

Figure 6. Event tree model for calculation $P(B/\overline{A})$

After calculation of the required conditional probability we will get the following expression for BIT uncertainty:

$$\overline{D} = P(A)P(\overline{C}_{fa}) + P(\overline{A})(P(\overline{C}_{no}) + (1-\eta)P(C)) \quad (10)$$

If BIT isolates two or more LRUs when only one LRU has failed, then probability of this event should be included in $\overline{D}$

$$\overline{D} = P(A)P(\overline{C}_{fa}) + P(\overline{A})(P(\overline{C}_{no}) + (1-\eta)P(C)) + P(\overline{A})\eta(1-\gamma_1)P(C) \quad (11)$$

3 TESTABILITY ORIENTED FAILURE MODE AND EFFECT ANALYSIS

Failure Mode and Effect Analysis (FMEA) is one of the most widely used tools for developing quality design. For the purpose of testability assessment we have used design detailed FMEA, applying some provisions of US MIL-STD-1629. Task 101, Task 102. Analysis was performed using inductive bottom-up approach starting the analysis with the failure modes at the LRU level and then successively iterating throw the levels of functional subsystems ending at the system level.

The main fields of FMEA worksheets, constructed for testability analysis, are presented in Table 1. Structured in such a way FMEA data were used to calculate the above indices Eqs. (5,6,11). The indices are calculated for each functional avionic subsystems and aircraft in general. Field FDM corresponds to the list of methods – CBIT (continuous BIT), PBIT (power-on BIT) and so on. Inclusion in this field of "none" item (the failure mode is not detected) makes it possible to calculate percent detection index Eq. (4).

Table 1. Main fields of FMEA worksheets

Field Name	Description
ID	LRU identifier. for example ATA code.
Name	LRU name and description
MTTF	LRU Mean time to failure
FM	LRU Failure Modes
FMP	Percent of each failure modes
FDM	Failure detection method
FID	Fault isolation descriptor – the list of LRUs ID, isolated by BIT
FMS	The LRU's failure mode severity
FMM	Mission Phase

4 CONCLUSION

We have presented unified approach to testability analysis of avionic systems at design stage. FMEA information was used as input data for testability evaluation. Calculation equations for computing BIT percent detection and isolation are described. Complex measure of BIT performance, viz BIT certainty, was suggested. This measure takes into account both fault detection and isolation characteristics and false alarm and "nonoperate" modes of BIT possible failures. Modification of standard FMEA worksheets was done for adaptation for the testability indices calculation. Markov reliability model for imperfect fault coverage and special strategy of avionic systems repair was constructed. It was shown that BIT behavior is a very important factor, which has a tremendous impact on the reliability of the avionic systems.

Described approach was applied in the study of testability of functional systems of Russian aircraft Sukhoi Superjet 100, developed by the Sukhoi Civil Aircraft Company, Moscow.

5 ACKNOWLEDGEMENT

Authors would like to thank and acknowledge the support of this work provided by management and staff of Sukhoi Civil Aircraft Company (CJSC), especially Pimenov A.V., Vedernikov B.I., Umashev V.G., Gangan Y.G. Authors appreciate Petrova N.A. from Tesabiliy Department of IRCUT for her great work on FMEA data structuring.

6 REFERENCES

Gnedenko, B.V., Belyaev, Yu. K., Solovyev, A.D. (1969). *Mathematical. Methods of Reliability Theory*. New York: Academic Press.

Kumamoto H., Henley E.J. (2000) *Probablistic Risk Assessment and Management for Engineers and Scientists.* John Wiley & Sons.

Victorova, V.S., Vedernikov B.I., Spiridonov I.B., Stepanyants A.S. (2007). Testability simulation and analysis of on-board aircraft systems. *Reliability Journal*, vol. 3 (22), pp. 62-71.

Victorova, V.S., Stepanyants A.S. (2008). Models for test integrity evaluation of on-board systems. *Proceedings of the 8th International Scientific School "Modeling and Analysis of Safety and Risk of Complex Systems" (MASR 2008)*, (pp. 357-362), June 24-28, StPb.

Victorova, V. S., (2009). *Aggregation of reliability and safety models of complex technical systems*. Doctoral dissertation. Institute of Control Sciences (IPU RAN), Moscow, Russia. http://www.dissercat.com.