ESReDA 41st Conference 2011
Advances in Reliability-based Maintenance Policies
05-06 October 2011, La Rochelle, France

# Session N°4, Paper N°10
# Availability of redundant systems with imperfect fault detection

**Dr Pierre DERSIN, Alban PERONNE**
ALSTOM Transport Information Solutions, RAM Center of Excellence
Saint-Ouen, FRANCE
pierre.dersin@transport.alstom.com

## Abstract

*Fault tolerance is a key feature of highly-available systems, in aerospace, rail transport, telecommunications and other areas. It is usually achieved through redundancy. But redundancy management implies being able to detect a fault before the function is lost. Such a detection can be achieved by various means: on-line built-in self test (BIST), off-line interruptive built-in test, regular scheduled inspection with or without external test equipment, or opportunistic inspections upon occurrence of detected faults.*

*The objective sought is to model the impact of those various fault detection methods on system availability, so as to assess the trade-offs between performance and cost. This type of problem lies at the crossroad between Maintenance and Reliability Engineering.*

*At the heart of these investigations lies the notion of mean undetected fault time (MUFT). The longer that time, the higher is the risk of a total loss of function, thus the less efficient the fault tolerance.*

*Some new insights have been gained which the authors report in the present paper.*
*For instance, when the scheduled inspection periodicity is much smaller than the MTBF of one channel, and the failure rate is constant, the distribution of the fault detection time is uniform. Relations can also be obtained between the MTBF corresponding to detected faults in a single channel and the MUFT of the redundant system. For instance, if the undetected fault modes occur much more rarely than the detected ones, the mean fault detection time is equal to half the MTBF corresponding to detected fault modes.*

*In general, the methodology that has been followed is that of continuous-time Markov chains, with transitions weighted by various fault detection probabilities. It permits modeling the various fault detection and maintenance strategies, and thus to measure the impact of testability on system availability and service reliability.*
*The conditional probability distribution of fault detection time is characterized.*

*Yet, Markov models do imply assumptions on recovery time distributions which are not always met in practice, and stochastic Petri nets or semi-*

*Markov approaches are thus preferable in the general case. This more-general approach is briefly described.*

*The methodology is illustrated in the context of rail transport.*

**Keywords** – Testability, Detection; Redundancy, Markov, Petri

## Introduction

The availability of a redundant (fault-tolerant) system is determined not only by the reliability of its constituents, but also by the efficiency with which redundancy is managed: when a failure occurs, it must be detected, and the failed component replaced as quickly as possible.
The stochastic properties of the undetected fault time $(\mathrm{UFT})$, i.e. the time between the occurrence of a failure and its detection, have a strong influence on system reliability and availability.
The preferred way of accomplishing fault detection is through built-in self tests (BIST), i.e. built-in test equipment (BITE) transmits an alarm as soon as the item it monitors fails. As this solution is not always cost effective and because BITE is not perfect, not all failures are detected in this way. A complementary means of detection is scheduled inspections with external test equipment. Yet another avenue is, upon occurrence of failures that BITE does detect, to then inspect for other items that might have failed unnoticed.
In the first part of this paper, the probability distribution of the undetected fault time is studied in the maintenance strategy that combines BITE with scheduled inspections.
This conditional distribution (given that a fault has been detected during inspection) is found to follow a uniform law, when components have a constant failure rate and it can be assumed that inspections occur on average much more frequently than failures, the most usual situation.
As a result, under those assumptions, $\mathrm{MUFT}$ is equal to half the time between two successive inspections.
If component times to failure are distributed as a Weibull law, the result is generalized and the variance of the undetected fault time is characterized in terms of the Weibull shape parameter.
A general expression for $\mathrm{MUFT}$ for constant failure rate, without any other assumption, is also given
A Markov model is then presented for the scheduled inspection strategy and it is shown how sensitive system reliability is to the BITE's fault detection rate.
Another Markov model is then introduced to model the opportunistic detection policy, i.e. relying on detected failures to discover hidden failures. The previous result on $\mathrm{MUFT}$ is generalized and, under the assumption that detectable failures occur much more frequently than undetectable ones, the $\mathrm{MUFT}$ is shown to be equal to half the $\mathrm{MTTF}$ of detectable failures.
In general, $\mathrm{MUFT}$ ranges from 50% to 100% of that $\mathrm{MTTF}$, and special cases are studied corresponding to given ratios between the $\mathrm{MTTF}$ of detectable and undetectable failures.

A more-general Markov model takes into account the different possible test policies.
Finally, the knowledge that the conditional distribution of $\mathrm{UFT}$ is uniform and that Markov models require it to be modeled as exponential, points to the limitations of Markov models and serves as a rationale for using stochastic Petri nets if more accuracy is required.

## Conditional Distribution of Undetected Fault Time

*A. Problem Statement*

When built-in test equipment (BITE) has an imperfect detection rate, it is usual to complement it with regular, scheduled inspections.
If the redundant structure is found faulty upon inspection, it is useful to characterize statistically the time elapsed since the first failure took place. This is important in building predictive models for availability or service reliability, such as Markov models, as described below. That time, the "undetected fault time" ($\mathrm{UFT}$), is a random variable, and its expectation is the mean undetected fault time ($\mathrm{MUFT}$). Here one is dealing with the conditional probability distribution of that random variable, given that a fault has been discovered upon inspection.
Referring to Figure 1, denote $\mathrm{T}$ the inspection periodicity, i.e. the time between two successive scheduled inspections, and by $\mathrm{s}$ the random time of occurrence of the first failure in the redundant structure. The time of the previous inspection is denoted $0$.
Thus it is sought to characterize the conditional distribution of $(\mathrm{T}-\mathrm{s})$ given that the structure was found faulty when inspecting at time $\mathrm{T}$, or equivalently given that a failure took place between time $0$ and time $\mathrm{T}$.

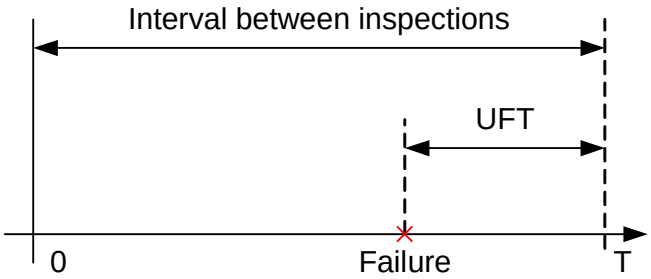


**Figure 1: Undetected Fault Time (UFT)**

By definition of the concept of conditional probability, that probability is given as follows, denoting by $\mathrm{F}(\mathrm{x})$ the cumulative distribution function of the random variable "time to first failure" of any one channel in the redundant structure.

$$\mathrm{P}[\mathrm{UFT} > \mathrm{x}] = \frac{\mathrm{F}(\mathrm{T}-\mathrm{x})}{\mathrm{F}(\mathrm{T})} \qquad \text{for } 0 \le \mathrm{x} \le \mathrm{T} \tag{1}$$

$$\mathrm{P}[\mathrm{UFT} > \mathrm{x}] = 1 \qquad \text{for } \mathrm{x} < 0$$

$$P[UFT > x] = 0 \qquad \text{for } x > T$$

For instance, in a KooN (K-out-of-N) redundant structure, $F(x)$ is the cumulative density function (CDF) of the time of the first failure among the N channels. If $R_1(x)$ denotes the reliability function for one channel (assuming all N channels are independent, identically distributed),

$$F(x) = 1 - R_1{}^N(x) \qquad (2)$$

One is interested here, not in the time to failure of the structure (which would imply the failure of at least K out of all N channels), but in the first failure time of any one of the N channels in the structure (which results in a failure that may go undetected depending on the detection rate of the built-in test equipment).

*B. Constant Failure Rate Case*

Let $\Lambda$ denote the combined intrinsic failure rate of all the channels that make up the redundant structure.

If all the n channels in the redundant structure have a constant failure rate $\lambda$, therefore an exponential time-to-failure distribution, then Equation 2 becomes, denoting $\Lambda = n\lambda$:

$$P[UFT > x] = \frac{1 - e^{\Lambda(T-x)}}{1 - e^{-\Lambda T}} \qquad \text{for } 0 \le x \le T \qquad (3)$$

$$P[UFT > x] = 1 \qquad \text{for } x < 0$$

$$P[UFT > x] = 0 \qquad \text{for } x > T$$

From Equation 3, the expression for $MUFT$ can readily be derived:

$$MUFT == \int_0^{\infty} P[UFT > x]dx = \int_0^{T} \frac{1 - e^{-\Lambda(T-x)}}{1 - e^{-\Lambda T}} dx$$

which yields

$$MUFT = \frac{T}{1 - e^{-\Lambda T}} - \frac{1}{\Lambda} \qquad (4)$$

*C. Weibull Case*

If all the channels in the redundant structure have a Weibull distributed time to failure (assuming the same scale parameter $\eta$ and shape parameter $\beta$), then the $UFT$ conditional distribution is given by:

$$P[UFT > x] = \frac{1 - e^{-N\left(\frac{T-x}{\eta}\right)^{\beta}}}{1 - e^{-N\left(\frac{T}{\eta}\right)^{\beta}}} \qquad \text{for } 0 \le x \le T \qquad (5)$$

$$P[UFT > x] = 1 \qquad \text{for } x < 0$$

$$P[UFT > x] = 0 \qquad \text{for } x > T$$

*D. Case of frequent Inspections*

In most cases of practical interest, the MTTF of each channel is much larger than the inspection periodicity: inspections are scheduled so as to take place "reasonably often" in relation to failure frequency. This situation translates into the following:

For the exponential distribution: $\lambda T << 1$
For the Weibull distribution: $T << \eta$

Under those conditions, Equation 3 and 4 considerably simplify:

$$P[UFT > x] = \frac{1 - e^{-N\left(\frac{T-x}{\eta}\right)^{\beta}}}{1 - e^{-N\left(\frac{T}{\eta}\right)^{\beta}}} \approx \frac{N\left(\frac{T-x}{\eta}\right)^{\beta}}{N\left(\frac{T}{\eta}\right)^{\beta}} = \left(1 - \frac{x}{T}\right)^{\beta} \quad (6)$$

to within higher-order terms in $T/\eta$.

In the special case of an exponential distribution $(\beta = 1)$, the conditional distribution of $UFT$ is a uniform distribution on the interval $(0, T)$. In other words, the failure detected at time $T$ is equally likely to have happened at any time since the last inspection. The conditional expectation is therefore given by:

$$MUFT \approx \frac{T}{2} \quad (7)$$

and the conditional variance is given by:

$$\sigma^2(UFT) \approx \frac{T^2}{12} \quad (8)$$

In the case of a Weibull distribution , the corresponding quantities are given by:

$$MUFT = \int_0^{\infty} R(x)dx \approx \int_0^{T} \left(1 - \frac{x}{T}\right)^{\beta} dx = \frac{T}{\beta + 1} \quad (9)$$

$$\sigma^2(UFT) \approx \frac{\beta}{(\beta+1)^2(\beta+2)} T^2 \quad (10)$$

(See Appendix 1 for the proof)

For $(\beta = 1)$, the expressions 7 and 8 for the exponential case are found again. Equation 7 is also found from Equation 4 by letting $\lambda T$ go to zero.

Equation 9 shows that, for increasing failure rate $(\beta > 1)$, $MUFT < T/2$ while, for decreasing failure rate $(\beta < 1)$, $MUFT > T/2$.

These results are consistent with intuition: in case of an increasing failure rate, the failure is more likely to have occurred recently; and the converse holds for a decreasing failure rate.

Equation 10 shows that the variance converges to $0$ when $\beta$ goes to infinity, which is consistent with the properties of the Weibull distribution. The maximum variance is reached for $\beta$ equal to $(\sqrt{5} - 1)/2 \approx 0.618$, as illustrated

in Figure 2. Thus, in the exponential distribution case, the variance of the UFT is greater than for any Weibull distribution with increasing failure rate.

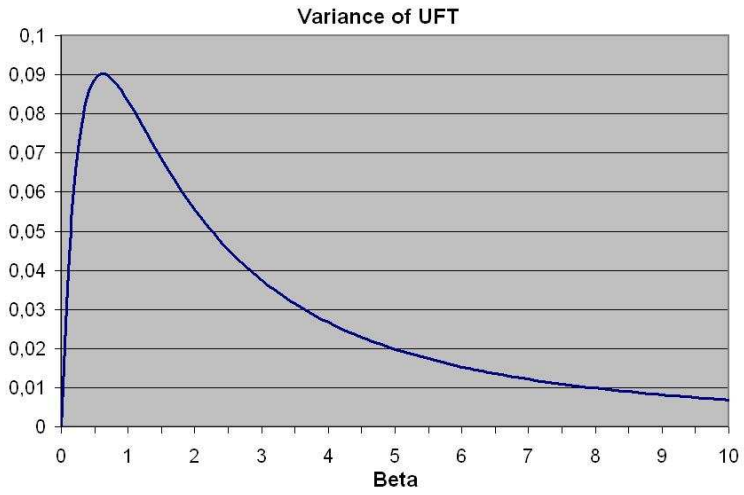


**Figure 2: Conditional Variance of Undetected Fault Time (Weibull)**

## Markov Modeling

*A. Imperfect detection (BITE and inspections)*

The key ideas behind Markov Models is to describe a system by means of the various states it can be in and the transitions which may lead from one state to another, then to calculate the probabilities of the system occupying each particular state at a given time.
It is assumed that, once the state is known, the past history of the system, i.e. how it got to that state, is irrelevant. Thus the future state is determined by the present state and the future transitions away from it, not by the past states.
Markov models are very useful and quite amenable to analytical treatment, their main limitation is the requirement that failure and restore rates be constant or, equivalently, that the times to transition from one state to another follow exponential distributions. This is in view of the memoryless property that characterizes Markov processes.
Figure 3 is the Markov model of a 1oo2 (one-out-of-two) redundant structure system, the fault detection (FD) capability of built-in test equipment and the "undetected fault time" (UFT) are modeled. Thus FD is the probability for a fault to be detected by the built-in self-test (BIST) when it occurs.

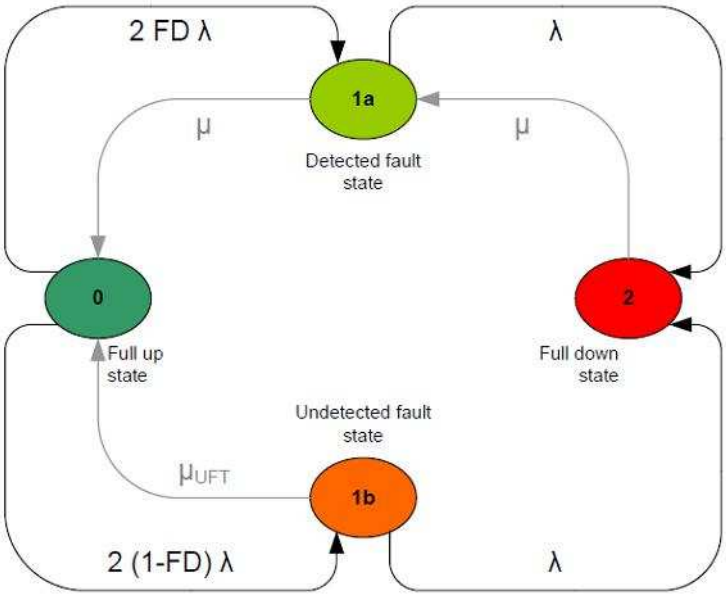


**Figure 3: System (1oo2) imperfect detection Markov model**

State 0 corresponds to system "Full up" state, there is no fault in any redundant items. State 1a corresponds to "Detected fault" state, one item is failed and the fault is detected. State 1b corresponds to "Undetected fault" state, one item is failed and the fault is undetected; as periodic online test inspections (at interval $\mathrm{T}$) are scheduled then the fault will be detected (UFT with exponential distribution of average MUFT is used).The corresponding restore rate is denoted $\mu_{UFT} = \frac{1}{\mathrm{MUFT}}$

State 2: corresponds to system "Full down" state, all redundant items are failed, the system is down.

One can then plot system MTTF as a function of fault detection $(\mathrm{FD})$ and inspection periodicity $(\mathrm{T})$ as shown in Figure 4.

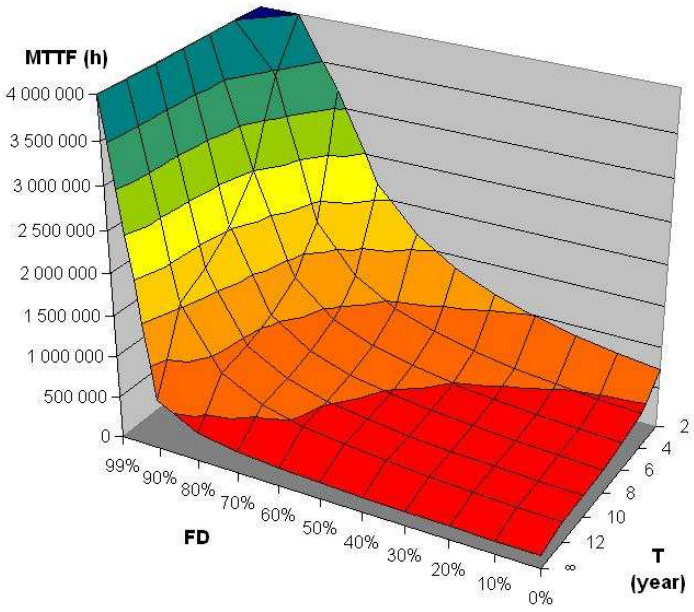


**Figure 4: System (1oo2) MTTF as a function of FD and T**

Solving the Chapman-Kolmogorov equations for the steady-state probabilities, it is possible to express the system MTTF as a function of FD and T (Figure 4). Not surprisingly, MTTF is an increasing function of FD and a decreasing function of T. The plot also shows that a lower testability must be compensated by more frequent inspections to retain the same system reliability. The sensitivity to FD is very high, as reported in [2].
This modeling technique is routinely used within ALSTOM Transport Information Solutions, in particular for the URBALIS® automated mass transit system where redundancies are very numerous in the automatic train control and data communication functions.

*B. Opportunistic detection*

Scheduled periodic inspections may be expensive and time-consuming. Some products are specified to be “maintenance-free”. In that case, another method can sometimes be envisaged: taking advantage of detectable failures (i.e. failures detected by BIST) in order to discover undetectable failures (i.e. failures missed by BIST). Figure 5 illustrates the concept symbolically on a 1oo2 (one-out-of-two) redundancy. Each item is assumed to consist of a portion whose failures are detectable [8] and a portion whose failures are not. When an undetectable failure takes place on one channel and it is followed by a detectable failure, two situations may arise:

- Either the two failures occur on different channels, in which case the second failure brings the system to a down state;
- Or the two failures occur on the same channel; then the second failure does not bring the system down but, when it takes place, the system can be subjected to a test and the first failure will be discovered. In other words the detectable failures trigger the inspections, which thus become random. We call this method “opportunistic detection”. The corresponding Markov graph is shown in Figure 6.

This method has been used within ALSTOM Transport Information Solutions for a trackside product where preventive maintenance is required to be minimal.

It is interesting to evaluate the conditional MUFT in the case of opportunistic detection, i.e. when a failure corresponding to the undetectable failure portion is discovered upon occurrence of a failure in the detectable failure portion.
This question is now addressed.

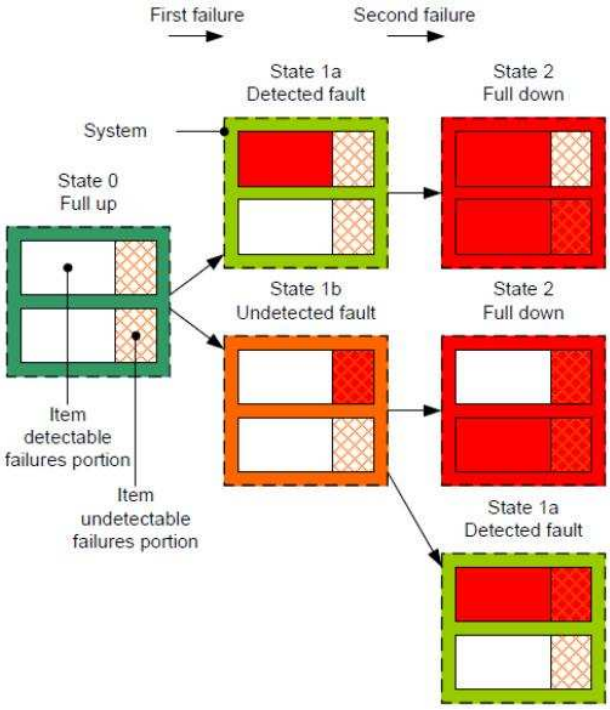


**Figure 5: System (1oo2) possible failure states and transitions**

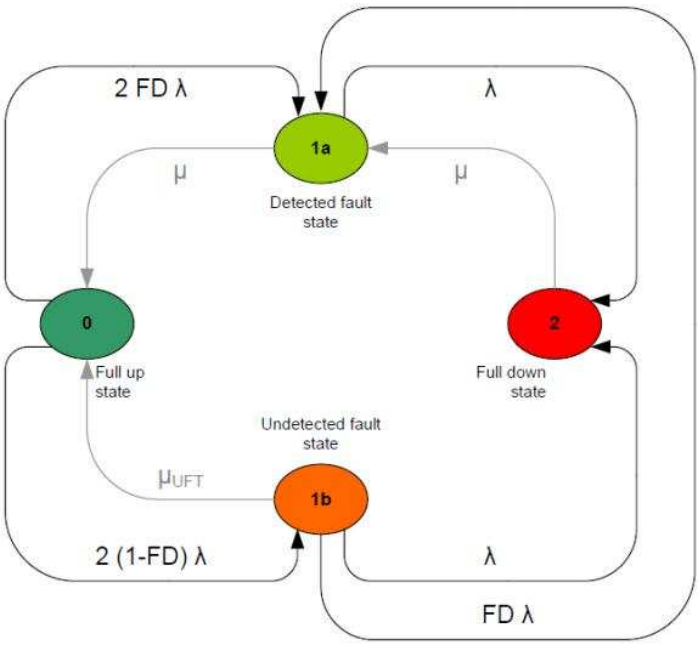


**Figure 6: System (1oo2) opportunistic detection Markov model**

From now on, $\lambda_1 = FD\lambda$ will denote the failure rate corresponding to the detectable failures, and $\lambda_2 = (1-FD)\lambda$ , that corresponding to the undetectable failures.

The previously obtained result on $MUFT$ (Equation 4) can be generalized by using conditional probabilities. Indeed, conditionally upon the value of the time of occurrence $T$ of a detectable failure, the probability distribution of $UFT$ is known: it is given by Equation 3, with $\lambda = \lambda_2$ and $N = 2$.

One then has to model $T$ as a random variable, distributed as an exponential distribution with parameter $\lambda_1$ (Note: $\lambda_1$ and not $2\lambda_1$ because one is modeling here the undetected fault time under the condition that a detectable failure takes place on the same channel as that where the undetectable failure took place i.e., the time to reach state 1a in Figure 6; if it happened on the other channel, the redundant system would reach a down state, i.e. state 2). Therefore:

$$P[UFT > x] = \int_0^\infty \frac{1-e^{-2\lambda_2(t-x)}}{1-e^{-2\lambda_2 t}} \lambda_1 e^{-\lambda_1 t} dt \qquad (11)$$

$MUFT$ can then be calculated as follows:

$$MUFT = E(UFT) = \int_0^\infty E(UFT \mid T = t)\lambda_1 e^{-\lambda_1 t} dt = \int_0^\infty \left( \frac{t}{1-e^{-2\lambda_2 t}} - \frac{1}{2\lambda_2} \right) \lambda_1 e^{-\lambda_1 t} dt \qquad (12)$$

Let us perform a change of variable by setting:

$$u = e^{-\lambda_1 . t} \qquad (13)$$

Then there follows from (12) that:

$$MUFT = E(UFT) = -\int_0^1 \frac{\log u}{\lambda_1 \left(1 - u^{2\frac{\lambda_2}{\lambda_1}}\right)} du - \frac{1}{2\lambda_2} \qquad (14)$$

*Special case when detectable failures are much more frequent than undetectable ones*

It was seen earlier that, when scheduled periodic inspections are performed, the usual case where inspection frequency is much higher than the frequency of failures $(\lambda T << 1)$ leads to a simplification and , in that case, $MUFT$ is very well approximated by half the inspection interval, $T/2$ (to within higher order terms in $\lambda T$).

When dealing with opportunistic detection, instead of comparing $\lambda$ with $1/T$, one must instead compare $\lambda_2$ with $\lambda_1$, i.e. the failure rate corresponding to undetectable failures with the failure rate of detectable failures. The equivalent condition to $\lambda T << 1$ is $\lambda_2 << \lambda_1$ , i.e. detectable failures are assumed much more frequent than undetectable ones. Under that condition, we shall now show that

$$MUFT \approx \frac{1}{2\lambda_1} \qquad (15)$$

Let us set: $x = \frac{2\lambda_2}{\lambda_1}$

Equation 14 can equally be written as:

$$MUFT = -\frac{1}{\lambda_1}\int_0^1 \left( \frac{\log u}{(1-u^x)} + \frac{1}{x} \right) du \qquad (16)$$

What is sought is the limit of $MUFT$ when $x$ goes to $0$. The limit and integral sign can be interchanged, therefore:

$$\lim_{x\to 0} MUFT = -\frac{1}{\lambda_1}\int_0^1 \lim \left( \frac{\log u}{(1-u^x)} + \frac{1}{x} \right) du$$

Noting that:

$$1-u^x = 1-e^{x\log u} = 1-\left(1 + x\log u + \frac{x^2 \log u^2}{2!} + \frac{x^3 \log u^3}{3!} + ...\right) = -\left(x\log u + \frac{x^2 \log u^2}{2!} + \frac{x^3 \log u^3}{3!} + ...\right)$$

for given $u$, the integrand is equal to:

$$\frac{\log u}{(1-u^x)} + \frac{1}{x} = \frac{\log u}{-\left(x\log u + x^2\frac{\log u}{2!} + x^3\frac{\log u^3}{3!} + ...\right)} + \frac{1}{x} = \frac{1}{x}\left(1 - \frac{1}{1 + \frac{x\log u}{2!} + \frac{x^2 \log u^2}{3!} + ...}\right)$$

and, for $x$ very small, this expression is equivalent to:

$$\frac{1}{x}\left(1-\left(1-\frac{x\log u}{2!} + o(x)\right)\right) = \frac{\log u}{2} + o(x)$$

Therefore,

$$\lim_{x\to 0} MUFT = -\frac{1}{\lambda_1}\int_0^1 \left( \frac{\log u}{(1-u^x)} + \frac{1}{x} \right) du = -\frac{1}{\lambda_1}\int_0^1 \frac{\log u}{2} du = \frac{1}{2\lambda_1}$$

*Other special cases*

Other cases where a closed form can be obtained are:

Case 1: $\lambda_2 = \frac{\lambda_1}{2}$, case 2: $\lambda_2 = \lambda_1$ and case 3: $\lambda_2 >> \lambda_1$

Case 3 is the opposite situation of the one examined earlier: the undetectable failures are much more frequent than the detectable ones.

$$\lim_{\frac{\lambda_2}{\lambda_1}\to\infty} MUFT = -\int_0^1 \frac{\log u}{\lambda_1} du - \frac{1}{\lambda_2} = \frac{1}{\lambda_1} - \frac{1}{\lambda_2} = MTTF_1 - MTTF_2 \approx MTTF_1$$

This result resembles, for scheduled inspections, the case where the inspections are much less frequent than the failures: $T >> 1/\lambda$. Then the $MUFT$ is virtually equal to $T$, the inspection periodicity.

Case 1: $\lambda_2 = \frac{\lambda_1}{2}$,

$$\mathrm{MUFT} = -\int_0^1 \frac{\log u}{\lambda_1(1-u)}du - \frac{1}{2\lambda_2} = \frac{\pi^2}{6\lambda_1} - \frac{1}{\lambda_1} = \left(\frac{\pi^2}{6} - 1\right)\frac{1}{\lambda_1} \approx \frac{0.645}{\lambda_1} = 0.645\,\mathrm{MTTF} \quad (17)$$

(use has been made of the fact that $\int_0^1 \frac{\log u}{(1-u)}du = \frac{\pi^2}{6}$, see [4]).

Case 2: $\lambda_2 = \lambda_1$, detectable and undetectable failures are then equally frequent. The MUFT is then obtained as follows as a function of $\mathrm{MTTF}_1$:

$$\mathrm{MUFT} = -\int_0^1 \frac{\log u}{\lambda_1(1-u^2)}du - \frac{1}{2\lambda_2} = \left(\frac{\pi^2}{8} - \frac{1}{2}\right)\frac{1}{\lambda_1} \approx \frac{0.73}{\lambda_1} = 0.73\,\mathrm{MTTF}_1 \quad (18)$$

(use has been made of the fact that $\int_0^1 \frac{\log u}{(1-u^2)}du = \frac{\pi^2}{8}$, see [4]).

In Table1, the various results are summarized and compared with the corresponding values for $\mathrm{MUFT}$ in the case of scheduled preventive inspections. For instance, the case $\lambda_2 = \frac{\lambda_1}{2}$ corresponds, in the scheduled inspection policy, to: $\lambda T = \frac{1}{2}$

Then Equation 4 yields:

$$\mathrm{MUFT} = T\left(\frac{1}{1-e^{-1}} - 1\right) \approx 0.58T$$

The case $\lambda_2 = \lambda_1$ for opportunistic detection corresponds, in the scheduled inspection policy, to $\lambda T = 1$.

Then Equation 4 yields:

$$\mathrm{MUFT} = T\left(\frac{1}{1-e^{-2}} - \frac{1}{2}\right) \approx 0.66T$$

**Table 1: MUFT in two maintenance policies**

| $\frac{\lambda_2}{\lambda_1}$ | MUFT (opportunistic detection) | MUFT (scheduled inspections) |
|---|---|---|
| 0 | $\frac{1}{2}\frac{1}{\lambda_1}$ | $\frac{1}{2}T$ |
| $\frac{1}{2}$ | $0.645\frac{1}{\lambda_1}$ | $0.58T$ |
| 1 | $0.73\frac{1}{\lambda_1}$ | $0.66T$ |
| $\infty$ | $\frac{1}{\lambda_1}$ | $T$ |

In both policies, opportunistic and scheduled inspections, the MUFT ranges from half the inspection periodicity or half the mean time to failure of detectable failures to 100% of that value, as the ratio of undetectable to detectable failure frequencies increases from zero to infinity.

*C. Multiple tests detection*

So far two types of tests have considered: built-in self-tests (BIST) and off-line tests. Usually three categories of tests are considered [8]:

- A: Test during operation (on-line test)
- B: Test under test conditions, without external test equipment (off-line test)
- C: Test under test conditions, with external test equipment (off-line test)

Off-line tests cause operations to be interrupted.

This leads to defining three probabilities: $FD_A$, $FD_B$, $FD_C$, corresponding to detection by tests of categories A, B and C respectively; and a fourth, $FD_D$, the probability of non-detection.

A fault detection and a mean undetected fault time $(MUFT)$ can be associated with each test category. Figure 7 illustrates the Markov model of a 1oo2 redundant structure system, which includes the multiple tests detection and opportunistic detection. Opportunistic detection corresponds to transitions $1b-1a$, $1c-1a$, $1c-1b$, $1d-1a$, $1d-1b$, and $1d-1c$.

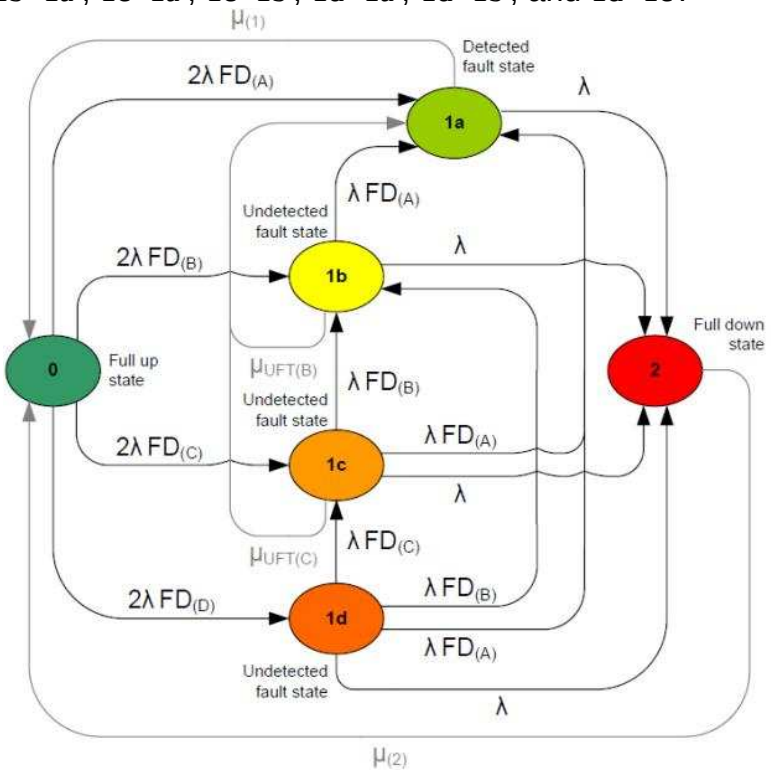


**Figure 7: System (1oo2) multiple tests and opportunistic Markov model**

## Petri Modeling

It was pointed out in the beginning of this paper that, in the frequent case when inspections are much more frequent that failures, the conditional distribution of $\mathrm{UFT}$ given that a failure has been detected at inspection $\mathrm{T}$ is a uniform distribution in the interval $(0,\mathrm{T})$.

But, when a Markov model is adopted, as shown in Figure 7, it is necessary to model that random variable (conditional $\mathrm{UFT}$) as being exponentially distributed, with an expectation equal to $\mathrm{T}/2$.

Figure 8 illustrates the difference between the two distributions. In particular, while the (true) uniform distribution of the conditional $\mathrm{UFT}$ guarantees it to be less than or equal to $\mathrm{T}$, the exponential distribution ranges from $0$ to infinity.

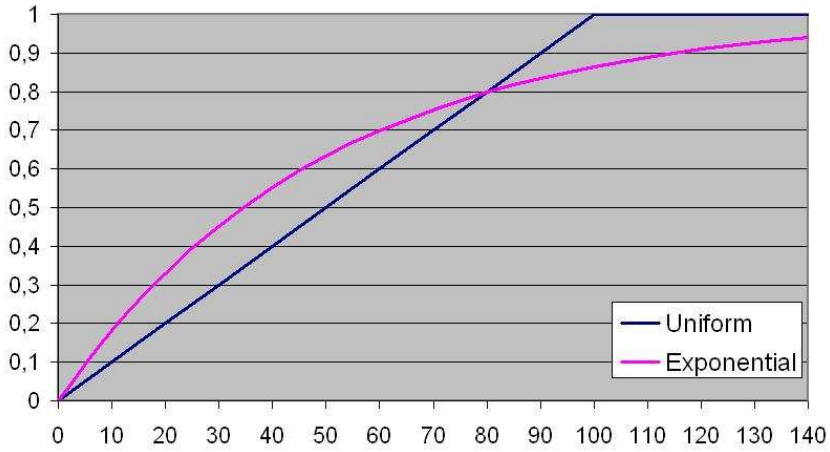


**Figure 8: Comparison of exponential and uniform distribution for UFT**

Figure 8 shows the cumulative distribution function $\mathrm{P}[\mathrm{UFT} < \mathrm{x}]$ ($\mathrm{T} = 100$ in this example)

It is seen from the Figure that, for values less than approximately $0.8\mathrm{T}$, the exponential distribution tends to underestimate the true value, while it tends to overestimate it for values above $0.8\mathrm{T}$.

Though the $\mathrm{UFT}$ as modeled in the Markov model has the same expectation as the true $\mathrm{UFT}$, it has a different distribution and in particular a higher variance: $\mathrm{T}^2/4$ instead of $\mathrm{T}^2/12$ for the uniform distribution.

Thus inaccuracies in the corresponding availability predictions will occur as a result. In order to escape the limitation of having to model $\mathrm{UFT}$ by an exponential distribution, one may use a more-general modeling technique: stochastic Petri nets (see e.g. [1]).

A stochastic Petri Net corresponding to the Markov model of Figure 5 is shown in Figure 9. In Figure 9, a token occupies Place 0, i.e. the current situation is “fully operational”. Comparisons between Markov and Petri Net approaches have been reported in [2] and [3].

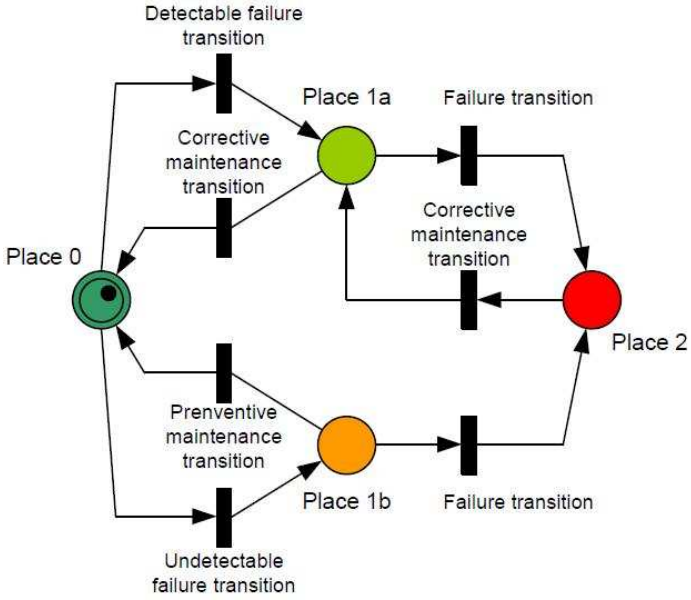


**Figure 9: System (1oo2) imperfect detection Petri nets model**

## Summary & Conclusion

Adequate testability is key to achieving high availability in fault-tolerant redundant systems.
Effective testability can be achieved through a combination of built-in self tests, scheduled inspection and what has been named in this paper opportunistic detection, i.e. taking advantage of detectable failures to discover hidden ones.
Testability parameters - typically fault detection probabilities in various test strategies - can be explicitly modeled in calculating system reliability and availability. A convenient way of doing so is through Markov models.
Then the mean undetected fault time $(\mathrm{MUFT})$ corresponding to scheduled inspections or opportunistic inspections must be used as a parameter in the model. In the case of scheduled inspection, it was seen that the best choice was to take $\mathrm{MUFT}$ equal to half the inspection periodicity (provided component failure rate can be assumed constant and much smaller than inspection frequency). A generalization of this property was given for opportunistic detection. But Markov models impose to model the undetected fault time $(\mathrm{UFT})$ with an exponential distribution when in fact it is uniformly distributed. More accurate models can be built, for instance with stochastic Petri nets.
Future research might focus on evaluating upper bounds on errors arising from the Markov approximation. Also the probability distribution of $\mathrm{UFT}$ in the opportunistic detection policy could be characterized.

## References

*[1] Birolini A., "Reliability Engineering: Theory and Practice" 6th Ed., Springer, New York, 2010*
*[2] Dersin P., Péronne A., Arroum C. (2008), "Selecting Test & Maintenance Strategies to achieve Availability Target at lowest Life-cycle Cost", 54th Annual Reliability & Maintainability Symposium (RAMS), Las Vegas, NE.*
*[3] Dersin P., "Achieving Availability cost-effectively in complex Systems"; Tutorial, 57th Annual Reliability & Maintainability Symposium, Orlando, FL.*
*[4] CRC Mathematical Tables, 20th Edition, 1972.*
*[5] Nachlas J., Reliabilty Engineering - Probabilistic Models and maintenance methods, Taylor & Francis, 2005*
*[6] Gertsbakh I., "Reliability Theory - with applications to preventive maintenance", Springer, 2000.*
*[7] IEC 60050-191, "Dependability Vocabulary", Ed. 1*
*[8] IEC 60706-5 "Maintainability of equipment - Part 5: Testability and diagnostic testing".*

## Appendix: Variance of UFT for a Weibull distribution

We set out to prove Equation 10. By definition,

$$\sigma^2(\mathrm{UFT}) = \int_{\grave{a}}^{\infty} (x-m)^2 f(x)dx \qquad \text{(A1)}$$

where $m$ denotes the expectation, $m = \mathrm{MUFT}$, and $f(\,)$ is the probability density of $\mathrm{UFT}$.
In the "frequent inspection" approximation,

$$m \approx \frac{T}{\beta+1} \qquad \text{(A2)}$$

and the reliability function is given by:

$$R(x) \approx (1-\frac{x}{T})^{\beta} \qquad \text{for } 0 \le x \le T \qquad \text{(A3)}$$

according to Equations 6 and 9.

Therefore the probability density is given by:

$$f(x) = -\frac{dR}{dx}(x) = \frac{\beta}{T}(1-\frac{x}{T})^{\beta-1} \qquad \text{(A4)}$$

Then Equation A1 can be written as:

$$\sigma^2(\mathrm{UFT}) = \frac{\beta}{T}\int_0^T (x-\frac{T}{\beta+1})^2 (1-\frac{x}{T})^{\beta-1}dx \qquad \text{(A5)}$$

Setting: $u = \frac{x}{T}$ ,

this is equivalent to:

$$\sigma^2(\mathrm{UFT}) = \beta T^2 \int_0^1 (u-\frac{1}{\beta+1})^2 (1-u)^{\beta-1}du \qquad \text{(A6)}$$

Using the fact that:

$$\int_0^1 x^{m-1}(1-x)^{n-1}dx = \frac{\Gamma(m)\Gamma(n)}{\Gamma(m+n)}$$

and expanding

$$(u-\frac{1}{\beta+1})^2 = u^2 - \frac{2}{\beta+1}u + \frac{1}{(\beta+1)^2},$$

Equation A6 becomes:

$$\sigma^2(UFT) = \beta T^2\left(\frac{\Gamma(3)\Gamma(\beta)}{\Gamma(\beta+3)} - \frac{2}{\beta+1}\frac{\Gamma(2)\Gamma(\beta)}{\Gamma(\beta+2)} + \frac{1}{(\beta+1)^2}\frac{\Gamma(1)\Gamma(\beta)}{\Gamma(\beta+1)}\right)$$

(A7)

Then using the fact that $\Gamma(x+1) = x\Gamma(x)$, Equation A7 simplifies into:

$$\sigma^2(UFT) = \frac{\beta}{(\beta+1)^2(\beta+2)}T^2$$

which is Equation 10.