An Investigation of the Reliability Performance of a System That is Guarded by a Responsive System of Protection

I. Vencel
Department of Engineering Physics
McMaster University
Hamilton, Ontario L8S 4M1

Supervisor: **Dr. William Garland**

Introduction

In this paper we will use the name *safety systems* to denote specially designed systems that serve to increase the efficiency or extend the lifetime of the system they were designed to protect. The type of connectivity between the safety system and the system it protects plays an important role in the performance of the compound system. Figure [1] represents a typical safety system together with its operating environment. This environment consists of

1. A system, or function that is to be protected (block named "MAIN SYSTEM")
2. A signal, or function that is to be protected from (block named "INITIATOR")
3. The safety system itself (block named "SAFETY SYSTEM"), and
4. Links between the blocks (connection protocols)

Figure 1. Safety System and Its Surroundings

Safety system serves as an interface between the main system and the initiator, and is designed to respond to a signal from the initiator and to protect the main system. Occasionally the safety system may become unavailable, and as a result its average performance is reduced in comparison to an ideal safety system that cannot fail. In some cases, however, it is possible to link the safety system and the main system in such a way that, regardless of the state of the initiator, the main system switches from an operating to a suspended state whenever the safety system becomes unavailable – either in full or in part. In general, this is feasible if the main system is not "mission-critical" and if the overall cost/benefit ratio requirements are fulfilled. All blocks on Figure [1] may represent technological as well as non-technological (human) systems and must be considered in their proper context when associating them with a particular function. For example, in order to prevent the initiator of bypassing the safety system, an airplane flight

may be canceled if the maintenance crew is on strike regardless of the aircraft condition. However, if the pilot during the flight suffers a stroke, the safety system is bypassed since the system has entered the mission critical phase and thus may not be suspended. In these two cases the main systems, which include aircraft, passengers, and crew, are identical, the safety systems are different, and the initiators are intercrossed. This is depicted on Figure [2] where “SS A” represents the maintenance crew, and “SS B” represents the cockpit crew. The “defense in depth” is said to be attained if the main system is guarded against a particular initiator by multiple safety systems. In our case such an initiator is an engine failure, denoted by “INIT B” on Figure [2]. “SS B” is a mission critical part, while “SS A” is a non-mission critical part of the safety system.

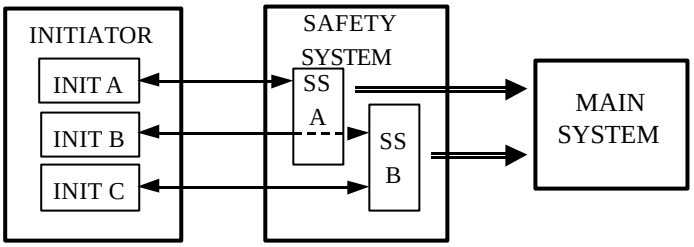

Figure 2. Arrangement of the Safety System Components in Case of the “Airplane Flight” Example

We want to show that the performance of the safety system capable of altering explicitly the state of the main system may be enhanced significantly in comparison to the performance of the identical safety system that cannot alter explicitly the state of the main system. In the case of the redundantly designed safety system better improvement in performance can be achieved by allowing the main system to be suspended when one of the redundant safety units fails to pass the test from the supervising unit (see Figure [3]). The safety system in this case remains fully operational. Thus, the tests are necessary. Compared to the power reactors, the advantageous cost/benefit considerations in the case of research reactors play an important role in terms of operational safety. Any detected fault in the safety system of a research reactor in general can and should be followed by the reactor shutdown. The reactor then should remain in the suspended state until the repair is done.

It should be noted that the two cases mentioned above – with and without the capability of altering the state of the main system - differ in the communication protocol between the safety and the main system, and not necessarily in the design of either the safety or the main system alone. In addition, the blocks depicted on Figure [1] do not necessarily represent physical objects. Since the main system may fail because of external as well as internal causes, the initiator may ‘physically’ reside outside as well as inside the main system. Figure [3] depicts a (redundant) safety system that is capable of altering explicitly the state of the main system. We will call this compound system the “Responsive System of Protection” (henceforth RSP), emphasizing the fact that the safety

system rather than the main system is the focus of our investigation. Nevertheless, it is the main system and not the safety system that will determine whether the compound system may or may not operate in the RSP mode.

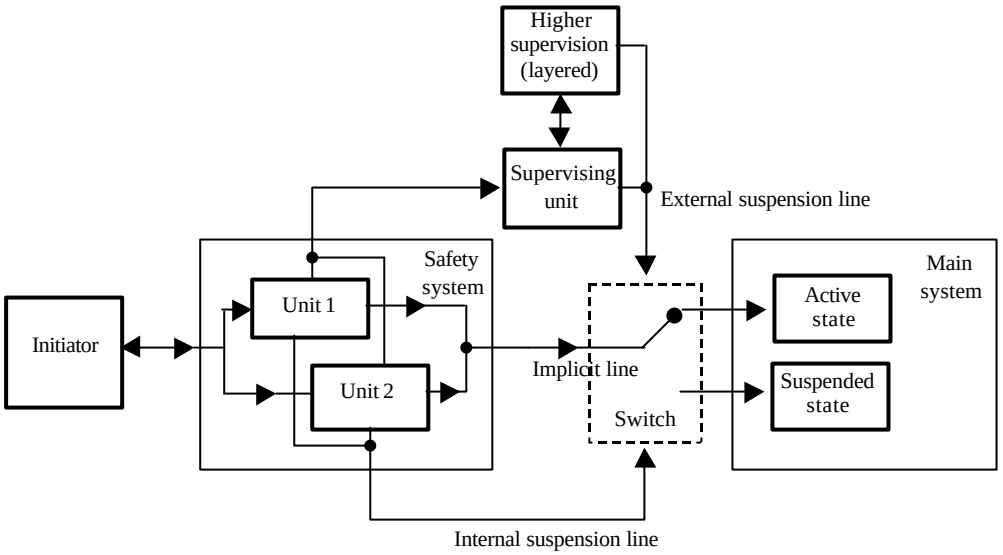

Figure 3. Responsive System of Protection (RSP)
Utilizing Two Redundantly Connected Safety Units

In the discussion to follow it is assumed that a safety system is redundant, consisting of two identical active parallel units. λ represents the failure rate of one unit, and μ represents the repair rate of one unit. λ^* represents the rate of failure of both units simultaneously and τ is the time between the tests. Since the actual repair of the RSP safety system is performed while the main system is in suspended state only, the mean repair time μ^{-1} in this case represents the expected time between the failure of a unit and the first subsequent scheduled test of the unit (see Figure [4]). Thus, the mean repair time is the time span between the actual failure and the detection of the failure. Without a loss of

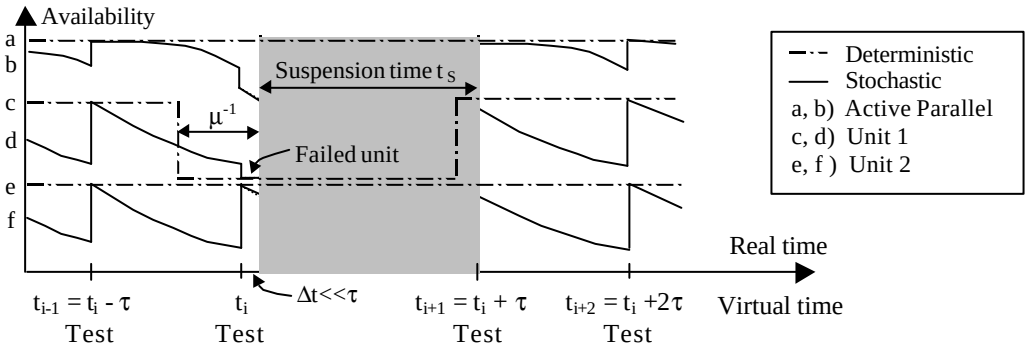

Figure 4. Timeline Diagram of RSP with Two Active Parallel Safety Units

generality, we may assume no delay in the transition of the RSP main system from active to suspended state once the failure of any of the safety units is detected. Hence, the 'effective' repair rate (μ) of any of the safety units becomes a function of both failure rates of the unit (λ, λ^*) and the rate at which the test of the unit is performed (τ^{-1}). Although we cannot change the failure rates, by increasing the test rate we can alter the effective repair rate of the RSP safety system and thus increase its availability. If we assume that the units of the safety system cannot fail simultaneously, the availability of the redundant RSP safety system can be, in fact, brought arbitrarily close to unity. Clearly, the definition of the effective repair rate allows us to incorporate the tests, which are essentially deterministic events, into the memoryless stochastic transition rates, and thus to analyze the system transitions using the markov modeling techniques.

Calculation of the Availability of the RSP Safety System

In the case of a safety system that is allowed to alter the state of the main system, it is feasible to maximize the availability of a particular cut set of the RSP at the cost of sacrificing the continuity of the main system's operation. (For the definition of the cut set see Barlow-Prochan, 1975.) This is, for example, the case of the McMaster Nuclear Reactor (MNR) Safety Amplifier, a part of the MNR's safety system, where the system can be brought down at any time when any part of the Safety Amplifier is suspected to be inoperable.

Let Ω_i be the sample space representing the state of unit *i* in the safety system. We only want to know whether the unit is working, so we may put Ω_i={"unit *i* is working", "unit *i* has failed"}, or succinctly $\Omega_i=\{W^i, F^i\}$. Let $t \in \mathfrak{I}^+$ denote a time in a future and $X_i(t): \Omega_i \times \mathfrak{I}^+ \rightarrow \{0,1\}$ be the stochastic process representing the pure failure of the unit 'i' at time 't', where '0' represents the working and '1' represents the failed state, and let 'n' be the number of units in the safety system. As already indicated, the expectation of the time interval between the moment of failure, i.e. the time when the transition from the pure state $X_0=\{W^1,\ldots,W^n\}$ to the markov state $X_j = \cap\{\mathbf{w}=(\omega_1,\ldots,\omega_n), \omega_i \in \Omega_i \mid X_1+\ldots+X_n=j\}$ occurs, and the time when the information of the failure becomes available to the observer plays the role of the effective repair time $E(\Delta t_{eff}(X_j)) = \mu^{-1}(j \rightarrow 0)$ for the state X_j, $j \neq 0$. When the failure is detected, the main system is automatically suspended until the repair is completed.

The case we want to analyze includes

1. actual repair during system shutdown only
2. repair during up time replaced by checkout procedures
3. possible external common cause (CCF) failures

A system that is shutdown is assumed to be in a suspended state, and does not count as a down time.

Repair rates $\mu(\lambda,\lambda^*,\tau)$ for the system with $(\lambda+\lambda^*)\tau \ll 1$ can be determined from the following proposition that will be proven separately:

Proposition 1.

$$\lim_{\lambda(1\to 2)\to 0} \frac{[\mu(2\to 0)](\lambda,\lambda^*,\tau)}{[\mu(1\to 0)](\lambda,\lambda^*,\tau)} = \frac{3}{2} \qquad (1)$$

Proposition [1], in the case of rare failures, yields the asymptotic value of the repair rate for "both units down" case relative to the "one unit down only" case. Only "both units down" will cause the safety system to fail. Proposition states that the ratio between the two (virtual) repair rates does not depend on failure rates (λ,λ^*) nor on the testing frequency τ. This gives the following transition rates for the system with frequent checkouts, i.e. for systems with $(\lambda+\lambda^*)\tau \ll 1$:

$\lambda(0\to 1) = 2\lambda$	$\lambda(1\to 2) = \lambda+\lambda^*$	$\lambda(0\to 2) = \lambda^*$
$\mu(1\to 0) = \mu$	$\mu(2\to 1) = 0$	$\mu(2\to 0) = 3/2\mu$

The transition matrix is

$$\mathbf{M} = \begin{pmatrix} -(2\lambda+\lambda^*) & \mu & 3/2\,\mu \\ 2\lambda & -(\mu+\lambda+\lambda^*) & 0 \\ \lambda^* & \lambda+\lambda^* & -3/2\,\mu \end{pmatrix} \qquad (2)$$

Initially, both safety units are considered to be operational, so that the probability distribution $\mathbf{P}(t=0) = [\,P_j(0)]$ of the system being in state X_j is

$$\mathbf{P}(t=0) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \qquad (3)$$

The Laplace transform of the rate equations, $d\mathbf{P}(t)/dt = \mathbf{M}\mathbf{P}(t)$, is $s\mathbf{P}(s) - \mathbf{P}(0) = \mathbf{M}\mathbf{P}(s)$, or

$$\begin{aligned} sP_1(s) &= 1 - (2\lambda+\lambda^*)P_1(s) + \mu P_2(s) + \frac{3}{2}\mu P_3(s) \\ sP_2(s) &= 2\lambda P_1(s) - (\mu+\lambda+\lambda^*)P_2(s) \\ sP_3(s) &= \lambda^* P_1(s) + (\lambda+\lambda^*)P_2(s) - \frac{3}{2}\mu P_3(s) \end{aligned} \qquad (4)$$

Solutions of the algebraic equations (4) are

$$P_1(s) = \frac{s+\mu}{s(s+\lambda+\mu+\lambda^*)(s+2\lambda+\mu+\lambda^*)}$$

$$P_2(s) = \frac{2\lambda(s+\mu)}{s(s+\lambda+\mu+\lambda^*)(s+2\lambda+\mu+\lambda^*)} \tag{5}$$

$$P_3(s) = \frac{s\lambda^* + 2\lambda^2 + 3\lambda\lambda^* + \mu\lambda^* + (\lambda^*)^2}{s(s+\lambda+\mu+\lambda^*)(s+2\lambda+\mu+\lambda^*)}$$

The solutions for the state probabilities in time domain are

$$p_1(t) = \frac{\mu}{2\lambda+\mu+\lambda^*} + \frac{2\lambda+\lambda^*}{2\lambda+\mu+\lambda^*} e^{-(2\lambda+\mu+\lambda^*)t}$$

$$p_2(t) = \frac{2\lambda\mu}{(\lambda+\mu+\lambda^*)(2\lambda+\mu+\lambda^*)} - \frac{2(2\lambda+\lambda^*)}{2\lambda+\mu+\lambda^*} e^{-(2\lambda+\mu+\lambda^*)t} + \frac{2(\lambda+\lambda^*)}{\lambda+\mu+\lambda^*} e^{-(\lambda+\mu+\lambda^*)t} \tag{6}$$

$$p_3(t) = \frac{2\lambda^2 + 3\lambda\lambda^* + \mu\lambda^* + (\lambda^*)^2}{(\lambda+\mu+\lambda^*)(2\lambda+\mu+\lambda^*)} + \frac{2\lambda+\lambda^*}{2\lambda+\mu+\lambda^*} e^{-(2\lambda+\mu+\lambda^*)t} - \frac{\lambda+\lambda^*}{\lambda+\mu+\lambda^*} e^{-(\lambda+\mu+\lambda^*)t}$$

The limiting availability can be found as a non-transient, or asymptotic, probability of the system being in the operating state

$$A = \lim_{t\to\infty}(p_1(t) + p_2(t)) = \frac{\mu^2 + 3\lambda\mu + \mu\lambda^*}{(\lambda+\mu+\lambda^*)(2\lambda+\mu+\lambda^*)} \tag{7}$$

The limiting unavailability is

$$U = \lim_{t\to\infty} p_3(t) = \frac{2\lambda^2 + 3\lambda\lambda^* + \mu\lambda^* + (\lambda^*)^2}{(\lambda+\mu+\lambda^*)(2\lambda+\mu+\lambda^*)} \approx \frac{2\lambda^2}{\mu^2} + \frac{\lambda^*}{\mu} = U_{Single} + U^* \tag{8}$$

The unavailability of the RSP safety system is approximately two times bigger than the unavailability of the similar system that: a) is incapable of suspending the main system; b) operates under external common cause failures; c) has two repairmen available; d) has the same reliability parameters as the RSP per each unit. Nevertheless, as opposed to the limited increase of the repair rates achievable by the repairmen in the mission critical case, the effective repair rates of the RSP safety system can be made almost arbitrarily

large by increasing the frequencies of the checkout procedures. This explains why the RSP model ultimately can accomplish better safety performance in practice.

The interval failure frequency $\varpi(t_1, t_2)$, defined as the expected number of times the system will fail in the time interval (t_1, t_2), can be calculated as

$$\varpi(t_1, t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} [p_1(t)\lambda^* + p_2(t)(\lambda + \lambda^*)]dt \tag{9}$$

Failure frequency ν is defined as the asymptotic value $\varpi(0, \infty)$, when this value exists. The failure frequency is

$$\begin{aligned} \varpi &= \lim_{T\to\infty} T^{-1}\varpi(0,T) = \lim_{T\to\infty} T^{-1} \int_{0}^{T} [p_1(t)\lambda^* + p_2(t)(\lambda + \lambda^*)]dt \\ &= \frac{\mu^2\lambda^* + \mu(\lambda^*)^2 + 2\lambda^2\mu + 3\lambda\lambda^*\mu}{(\lambda + \mu + \lambda^*)(2\lambda + \mu + \lambda^*)} = \mu p_3(\infty) \end{aligned} \tag{10}$$

The mean time between failures *MTBF* is equal to ϖ^{-1}. Taking into account only the predominant terms from the previous equation we have

$$MTBF = \frac{\mu}{2\lambda^2 + \mu\lambda^*} \tag{11}$$

In most cases of interest the external common mode failure rate λ^* satisfies the condition $\lambda^* \ll \varpi(\lambda^*=0)$, so that the *MTBF* simply becomes $(\lambda^*)^{-1}$, i.e.

$$\varpi(\lambda^* \ll \varpi(\lambda^* = 0)) = \lambda^* \tag{12}$$

Note that if we increase μ, then $\varpi \to \lambda^*$ even when $\lambda^* \ll \lambda$, i.e.

$$(\forall\delta > 0)(\forall\lambda > 0)(\forall\lambda^* > 0)(\exists M > 0)((\mu > M) \Rightarrow (\|\varpi(\mu, \lambda, \lambda^*) - \lambda^*\| < \delta)) \tag{13}$$

The convergence $\varpi \to \lambda^*$ takes place from right to left, or written in compact form: $\mu\uparrow \Rightarrow \varpi\downarrow\lambda^*$, meaning "if μ increases then ϖ approaches λ^* from the right (decreases)".

The failure frequency ϖ and *MTBF* are the same as for the mission critical case. However, as stated above, the expected duration of the safety system down time is twice as large, because of the unavailability differences. The following results for mission critical case suffices from the RSP case: 1) $\varpi(\lambda^* \ll \varpi(\lambda^*=0))=\lambda^*$; 2) $\mu\uparrow \Rightarrow \varpi\downarrow\lambda^*$.

Conclusion

According to cost/benefit calculations, the safety of a system may be increased, and thus the risk-associated cost reduced, at the expense of the increased cost of the more frequently performed tests of the safety components. This is not a serious disadvantage for experimental or research reactors because they do not produce revenues and,

consequently, any loss associated to the downtime is negligible. The expenditure associated with increased tests in terms of the increased operational cost is much smaller. In case of power reactors, on the other hand, any downtime is costly, and the shutdown is not always recommended. This is a safety drawback. As shown earlier, this safety variation is strictly connected to the mode of operation, i.e. reactor exploitation (profitable vs. non-profitable), and is not directly connected to the actual reactor design. The method we have used allow us to calculate, at least in principle, the maximum test rate that can reasonably be expected to cut down the unavailability to its limiting value below which the common cause failures will almost exclusively become responsible for any system failure. At this point no further safety improvement is achievable by increasing the testing frequencies.

Proof of the Proposition (1)

The reason why we used different letters for failure and repair rates, λ and μ, instead of just using $\lambda(i\to j)$ for both $i<j$ and $i>j$, is to indicate the difference in their nature: the failure transitions are spontaneous while the repair transitions are stimulated. In fact, both reliability and availability can be defined as (see Barlow-Prochan [1975])

$$A(t) = P[\phi(\mathbf{X}(t)) = 1] = E[\phi(\mathbf{X}(t))] \tag{14}$$

where $\mathbf{X}\equiv(X_1,\ldots,X_n)$ is a state vector of the system, E stands for mathematical expectation, and $\phi(\mathbf{X}(t))$ denotes a structure function. For definition of the structure function see Barlow-Prochan [1975]. In case of reliability, the stimulated transitions, or repairs, are forbidden.

From the principle of total probability it follows that the failure probability is

$$\begin{aligned} F(t) &= P(t = fail) \\ &= P(t = fail|\tau = fail)\cdot P(\tau = fail) \\ &+ P(t = fail|\tau = survive)\cdot P(\tau = survive) \end{aligned} \tag{15}$$

The shorthanded notation $t = fail$ means $\phi(\mathbf{X}(t)) = 1$. Hence, for $t<\tau$ the forbidden transition in the second term yields zero probability, and

$$\begin{aligned} F(t) &= P(t = fail|\tau = fail)\cdot F(\tau) + 0\cdot(1 - F(\tau)) \\ &= F(t|\tau = fail)\cdot F(\tau) \end{aligned} \tag{16}$$

Rearrangement gives the expression for conditional failure probability

$$F(t|\tau = fail) = \frac{F(t)}{F(\tau)} \tag{17}$$

Unlike reliability, failure probability is a distribution function and it generates the probability density f. Hence, the condition (17) transforms to the well-known equation

$$\langle t|\tau = fail\rangle = \frac{\int_0^\tau tf(t)dt}{\int_0^\tau f(t)dt} \tag{18}$$

The density of $F(t|\tau=fail)$ is

$$f(t|\tau = fail) = \begin{cases} \dfrac{f(t)}{\int_0^\tau f(t)dt} & if \quad 0 \le t < \tau, \\ 0 & if \quad \tau \le t \end{cases} \tag{19}$$

All failure rates can be derived heuristically and do not need special explanation. They are: $\lambda(0\to1)=2\lambda$, $\lambda(0\to2)=\lambda^*$, and $\lambda(1\to2)=\lambda+\lambda^*$. We will need them as well as Equation (19) in order to find the repair rates $\mu(1\to0)$ and $\mu(2\to0)$. As it is self-evident, $\mu(2\to1)$ is zero. We can calculate $\mu(1\to0)$ by using Equation (19) knowing that initially $p_0(0)=1$ (recall that the index below "p" indicates markov state: zero means "as good as new", and the variable in parentheses indicates time). However, after the transition $(0\to1)$ occurs at time *t*, the failed system at later time τ will not remain in a pure markov state since the transition $(1\to2)$ can occur spontaneously. That is why we should not use Equation (19) in terms of $\lambda(0\to1)=2\lambda$, but rather in terms of a conditional single unit failure disregarding the second unit that would, according to the condition at time τ, never undergo any transition anyway. The rigorous proof of this fact requires Bayes' theorem - it is trivial, but lengthy, and will be omitted herein. Therefore, for a single failure we have

$$\langle t|\tau = fail\rangle = \frac{\int_0^\tau t\lambda e^{-\lambda t}dt}{\int_0^\tau \lambda e^{-\lambda t}dt} = \frac{1-e^{-\lambda\tau}-\lambda\tau e^{-\lambda\tau}}{\lambda(1-e^{-\lambda\tau})} \tag{20}$$

and hence for $\mu(1\to0)$ we have

$$\mu(1\to 0) = [\tau - \langle t|\tau = fail\rangle]^{-1} = \lambda\cdot\frac{1-e^{-\lambda\tau}}{\lambda\tau + e^{-\lambda\tau}-1} \tag{21}$$

For $\lambda\tau \gg 1$ the following approximation can be derived

$$\lim_{\lambda\to0}\mu(1\to 0) = \frac{2}{\tau} \tag{22}$$

while for $\lambda\tau \ll 1$

$$\lim_{\lambda\to\infty}\mu(1\to 0)=\lim_{\lambda\to\infty}\frac{1}{\tau-\frac{1}{\lambda}}=\lim_{\lambda\to\infty}\frac{1}{\tau-MMTF}=\frac{1}{\tau} \tag{23}$$

We can interpret this as follows:

a) for frequent checkouts, or rare failures, the failure density remains constant throughout the checkout time window, so that in average the failure happens at the middle of the time interval between the checkouts (Equation (22));

b) for rare checkouts, or frequent failures, the failure will happen on average at time 1/λ after the previous checkout, and from the right side of the time window, i.e. at the time of the last checkout, this time appears to be close to the point of the previous checkout (Equation (23)).

Similarly, for a dual failure during time interval τ, i.e. for μ(2→0) calculation purposes, from λ(0→2)=λ* and λ(1→2)=λ+λ* we can calculate the exact system failure probability at time *t* taking into account dependencies as

$$P(0\to 2)(t)=F_{sys}(t)=1-2e^{-(\lambda+\lambda^*)t}+e^{-(2\lambda+\lambda^*)t} \tag{24}$$

which gives the probability density function as

$$f(t)=\frac{dF_{sys}(t)}{dt}=2(\lambda+\lambda^*)e^{-(\lambda+\lambda^*)t}-(2\lambda+\lambda^*)e^{-(2\lambda+\lambda^*)t} \tag{25}$$

Using the previous equation and Equation (18), we can find the conditional expectation of dual failure time counting from the end of the previous inspection. Consequently, the repair rate becomes

$$\begin{aligned}\mu(2\to 0)&=[\tau-\langle t|\tau=fail\rangle]^{-1}\\&=\frac{1-2e^{-(\lambda+\lambda^*)\tau}+e^{-(2\lambda+\lambda^*)\tau}}{\tau+\frac{2}{\lambda+\lambda^*}e^{-(\lambda+\lambda^*)\tau}-\frac{1}{2\lambda+\lambda^*}e^{-(2\lambda+\lambda^*)\tau}+\frac{1}{2\lambda+\lambda^*}-\frac{2}{\lambda+\lambda^*}}\end{aligned} \tag{26}$$

Hence

$$\lim_{(\lambda+\lambda^*)\to 0}\mu(2\to 0)=\frac{3}{\tau} \tag{27}$$

and

$$\begin{aligned}\lim_{(\lambda+\lambda^*)\to\infty}\mu(2\to 0)&=\lim_{(\lambda+\lambda^*)\to\infty}\frac{1}{\tau-\left[\frac{2}{\lambda+\lambda^*}-\frac{1}{2\lambda+\lambda^*}\right]}\\&=\lim_{(\lambda+\lambda^*)\to\infty}\frac{1}{\tau-MMTF}=\frac{1}{\tau}\end{aligned} \tag{28}$$

Therefore, for rare failures the dual failure time in mean is shifted from the middle point between the checkouts towards the latest checkout time (Equation (27)). Nothing is changed in terms of rare checkouts (Equation (28)). Finally, Equation (27) together with Equation (22) gives Equation (1).

References

[1] Barlow, Richard E., Prochan, Frank, 1975. “Statistical Theory of Reliability and Life Testing”, Holt, Rinehart and Winston, Inc.

[2] Grandell, Jan, 1991. “Aspects of Risk Theory”, Springer-Verlag New York Inc.

[3] Proceedings of the NATO Advanced Study Institute on Synthesis and Analysis Methods for Safety and Reliability Studies, 1978. “Synthesis and Analysis Methods for Safety and Reliability Studies”, held at SOGESTA Conference Centre, Urbino, Italy, July 3-14, 1978.

[4] Ross, Sheldon M., 1996. “Stochastic Processes”, John Wiley & Sons, Inc.

[5] Shiryaev A.N., 1996. “Probability” translated by R.P. Boas. New York, Springer.

[6] Sharpe, Michael, 1988. ”General theory of Markov processes”, Boston : Academic Press.

[7] Singh, Chanan, Billinton Roy, 1997. “System Reliability Modeling and Evaluation”, Hutchinson & Co. Ltd.