ELSEVIER

Journal of Hazardous Materials 142 (2007) 741–746

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

Updated hazard rate equations for dual safeguard systems

Marc Rothschild*

Rohm and Haas Company Engineering Division, 3100 State Road, Croydon, PA 19021, United States

Available online 3 July 2006

Abstract

A previous paper by this author [M.J. Rothschild, Updated hazard rate equation for single safeguards, J. Hazard. Mater. 130 (1–2) (2006) 15–20] showed that commonly used analytical methods for quantifying failure rates overestimates the risk in some circumstances. This can lead the analyst to mistakenly believe that a given operation presents an unacceptable risk. For a single safeguard system, a formula was presented in that paper that accurately evaluates the risk over a wide range of conditions. This paper expands on that analysis by evaluating the failure rate for dual safeguard systems. The safeguards can be activated at the same time or at staggered times, and the safeguard may provide an indication whether it was successful upon a challenge, or its status may go undetected. These combinations were evaluated using a Monte Carlo simulation. Empirical formulas for evaluating the hazard rate were developed from this analysis. It is shown that having the safeguards activate at the same time while providing positive feedback of their individual actions is the most effective arrangement in reducing the hazard rate. The hazard rate can also be reduced by staggering the testing schedules of the safeguards.

Keywords: Failure rate data; Hazard rate; Demand rate; Safeguard failure rate; Monte Carlo simulation; Multiple safeguards

1. Introduction

Hazards can occur when a demand is placed on a system that can lead to an adverse consequence, and the safeguard(s) that prevent or mitigate the consequence fail. The hazard rate is simply the frequency of the initiating event (the system demand) multiplied by the likelihood that the safeguard(s) are in a failed state upon demand:

$$\begin{aligned}&\text{hazard rate}\,(H)\\&\quad=\text{system demand rate}\,(D)\\&\qquad\times\text{safeguard in a failed state upon demand}\,(Q)\end{aligned}\tag{1}$$

The solution to this equation is easy to solve when the safeguard failure data is associated with the demand. However, the safeguard failure data is instead often given in the literature as a failure rate.[1] In these instances, this equation cannot be directly solved and alternative equation(s) must be used.

As presented in the "prequel" to this paper [1], the hazard rate in a given test interval for a single safeguard system is as follows:

$$H=\left(\frac{1}{T}\right)D\int_0^T(1-\mathrm{e}^{-\lambda t})\,\mathrm{d}t\tag{2}$$

where T is the test interval (time), D the system demand rate (demands per unit time), λ the safeguard failure rate (failures per unit time) and t is the time.

As discussed in that paper, the safeguard failure rate is dependent on the system demand rate; however, this dependency becomes negligible when the demand rate in per test interval is small ($DT \ll 1$). Furthermore, the term in the integration $(1-\mathrm{e}^{\lambda t})$ can be approximated as λt when for small values of λt. Since the longest period of time that a safeguard is in service is the testing interval (T), the above approximation applies when $\lambda T \ll 1$.

* Tel.: +1 215 785 7327.
E-mail address: mrothschild@rohmhaas.com.

[1] Technically speaking, all failures can take the form of "failure upon demand." When the cause of the failure is well defined and is something that can be measured, then the likelihood of failure upon that demand can be directly evaluated. For example, the rate that a pump fails to start can often directly be associated with the demand rate to start the pump, giving a direct correlation. Other times, however, there may be one or more causes that cannot be precisely identified and/or measured, so association of the failure with those causes is not feasible. However, from a macro view, the safeguard failures resulting from these undefined causes appear to occur randomly. An example of this is a pump failing while running. There are possibly many causes of pump failure during operation, with no one dominating cause. However, the combination of these causes results in an apparent random pattern. This failure data is recorded as the number of failures in a given time period, giving an effective failure rate.

0304-3894/$ – see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2006.06.116

Based on these two common approximations, Eq. (2) can be converted the well known equation given below:

$$H = D\left[\left(\frac{T}{2}\right)\lambda\right] \tag{3}$$

Comparing to Eq. (1), the term in the bracket is shown to be the likelihood that the safeguard is in a failed state, given a demand. When these simplifying assumptions apply, the hazard rate is shown to be directly proportional to the system demand rate, the testing interval, and the safeguard failure rate and that reducing any of these parameters would reduce the hazard rate. This equation shows that the existence of the safeguard in a failed state, by itself, does not result in a hazardous occurrence. Instead, to result in a hazard, a system demand must also occur while the safeguard is in a failed state. Since safeguards are tested and fixed, as needed, at each testing interval, the likelihood of a safeguard existing in a random failed state decreases with increased safeguard testing.

While the assumptions behind Eq. (3) are often valid, they are not always so. Eq. (3) does not apply when the failure rate or the demand rate is not very small. In that case the following more generalized equation, presented in the previous paper [1] applies:

$$H = \left[\frac{D\lambda}{D+\lambda}\right]\left\{\frac{1-(1-\mathrm{e}^{-(D+\lambda)T})}{(D+\lambda)T}\right\} \tag{4}$$

All of these formulas are based on the following conditions:

- The safeguard is tested offline at regular defined intervals, T;
- Safeguard failures and system demands are random;
- Safeguard failures go undetected ("hidden" failures) until there is either a demand or a test;
- Upon detection (either by a demand or a test), the safeguard is immediately repaired to perfect working order and returned to service (i.e., mean time to repair is taken as insignificant).

While the above equations are useful for evaluating the hazard rates for single safeguard systems, many systems are equipped with more than one safeguard. This paper presents useful formulas for evaluating the hazard rate for systems with two safeguards.

2. Dual safeguard systems

Operating with two independent safeguards reduces the likelihood of experiencing a hazardous event when a failure of either safeguard is sufficient to safely shut down the process. This is commonly referred to in the process industry as 1002 (one out of two) voting. However, not all 1002 systems are the same.

Two safeguards can be applied to activate in parallel or in series. An example of parallel safeguards is two high level switches, each set to activate at the same level. Two safeguards do not necessarily have to activate simultaneously to be classified as parallel safeguards, as long as both safeguards are challenged by the same demand. Series safeguards, on the other hand, activate at distinctly different time steps. A high level and a separate high-high level alarm is an example of two safeguards in series. To be classified as a series arrangement, successful operation of the first safeguard would prevent a challenge to the subsequent safeguard.

For a single safeguard system, failure of the safeguard would be detected by the demand (resulting in a "fatal" test). With multiple safeguards this is often – but not always – the case. The status of each safeguard when challenged is usually apparent when the safeguards are applied in sequence. An example of this would be a high-level shutoff set at 80% level, and a high-high level shutoff set at 90% level. If the filling operation is shut down by high level then, if the resulting level is 80%, it is clear that the first safeguard works; if the level is 90%, then it can surmised that the first safeguard has failed and the second one has worked (of course, if the tank overfills, then it is clear that both safeguards have failed!). The safeguard status is also usually apparent for different safeguard actions. An example of this situation would be two high level switches set to trip at the same height, with one switch closing an inlet valve, and the other shutting off the charge pump. Following a demand, the functional status of each of these safeguards would be apparent by the operational status of the equipment that they each activate. These safeguards are referred to in this paper as having detected failures.

In other safeguards arrangements, safeguards can be applied to operate coincidentally and provide identical information, so that the functional status of any individual safeguard cannot be determined from the overall operation (unless, of course, a hazard occurs, indicating failure of all of the safeguards). An example of this configuration might be two high level switches placed to activate at or near the same level, both shutting off the charge pump. In this case, the pump shutting down upon high level only indicates that at least one of the safeguards worked, but does not indicate the specific operational status of either safeguard. These safeguards are referred to as having undetected failures.

The failure rate for two safeguard systems depends on whether they are detectable or undetectable and, if the former, whether they are in parallel or in series. For detectable safeguards in parallel, both safeguards are challenged at each demand and the failure of both safeguards would be immediately apparent. In contrast, with a series arrangement, the failure of the backup safeguard would only be apparent if the first safeguard fails. This results in a longer time period between demands for this safeguard, increasing its likelihood of being in a failed state when needed. Either of the above detectable configurations is better than undetected failures.

3. Evaluating hazard rates for dual safeguard systems

In addition to the conditions given above for analyzing a single safeguard system, this evaluation of multiple safeguard systems is based on the following three conditions[2]:

[2] Real life, of course, is not constrained by these or the previous conditions. However, the analysis given in this paper is only valid when these conditions apply.

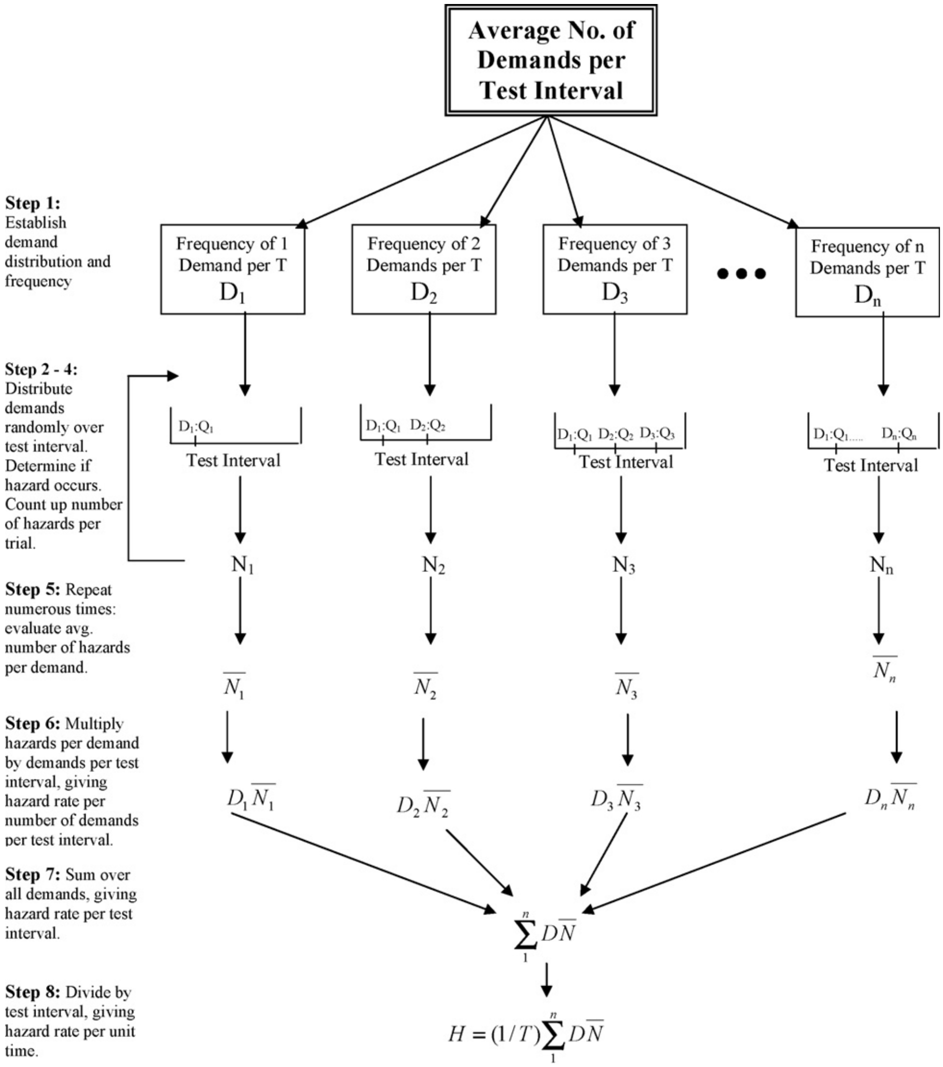
Average No. of Demands per Test Interval
Step 1: Establish demand distribution and frequency
Frequency of 1 Demand per T D_1
Frequency of 2 Demands per T D_2
Frequency of 3 Demands per T D_3
Frequency of n Demands per T D_n
Step 2 - 4: Distribute demands randomly over test interval. Determine if hazard occurs. Count up number of hazards per trial.
D_1:Q_1
D_1:Q_1 D_2:Q_2
D_1:Q_1 D_2:Q_2 D_3:Q_3
D_1:Q_1..... D_n:Q_n
Test Interval
N_1
N_2
N_3
N_n
Step 5: Repeat numerous times: evaluate avg. number of hazards per demand.
$\overline{N_1}$
$\overline{N_2}$
$\overline{N_3}$
$\overline{N_n}$
Step 6: Multiply hazards per demand by demands per test interval, giving hazard rate per number of demands per test interval.
$D_1\overline{N_1}$
$D_2\overline{N_2}$
$D_3\overline{N_3}$
$D_n\overline{N_n}$
Step 7: Sum over all demands, giving hazard rate per test interval.
$\sum_1^n D\overline{N}$
Step 8: Divide by test interval, giving hazard rate per unit time.
$H = (1/T)\sum_1^n D\overline{N}$

Fig. 1. Monte Carlo approach.

- The safeguards are tested concurrently;
- The two safeguards have the same failure rate;
- The safeguards do not share a common cause failure mode.[3]

If there is no more than one system demand in a test interval ($DT \ll 1$), then there effectively is no difference between detected and undetected systems since, following the demand, the safeguards will be tested before the next demand occurs. Likewise, since there is at most only one demand, then the time period between the previous test and the given demand is the same for both safeguards, whether they are in parallel or in series. Therefore, for a low demand rate, all safeguard systems provide the same level of protection.

If the safeguard failure rates are also small $\lambda T \ll 1$, then the hazard rate can be analytically solved as follows:

$$H = \frac{D}{T}\int_0^T (\lambda t)^2\,\mathrm{d}t = \frac{D\lambda^2 T^2}{3}, \quad \text{when } \lambda T \text{ and } DT \text{ are } < 0.1 \tag{5}$$

A Monte Carlo simulation was used to find the generalized solution for the hazard rate as a function of the demand and failure rates for the three distinct types of dual safeguard systems. In this approach, demands are randomly placed within a test interval, and the resulting system failures are counted. This is repeated numerous times to get a good statistical sampling,[4] giving in an average number of system failures. A further description of the Monte Carlo simulation method is found in Lees [2]. The following steps describe the Monte Carlo simulation, as depicted in Fig. 1.

[3] This may not be a realistic basis for many safeguards as similar safeguards will likely share a common mode failure. In other safeguard combinations, such as a high level switch paired with a weigh scale reading, the assumption of no common cause failure may be reasonable. If common cause failure is possible then, based on a 10% common cause factor, the actual failure rate would be around 10–20% higher than given in this analysis.

[4] As many as 600,000 trials were run.

(1) From the average demand rate per test interval (*DT*), the distribution and frequency of the discrete possible number of demands in a given test interval is determined, based on a Poisson distribution.
(2) For each select number of demands-per-test interval, the demands are randomly distributed within the test interval.
(3) For each demand, the conditional likelihood of failure of the associated safeguards is determined ($Q = 1 - e^{-\lambda\Delta t}$), where Δt is the time between the previous demand or test and the current demand. For each safeguard, this probability is compared with a random generated number between 0 and 1 (different random number for each safeguard). If Q is greater than the random number, then the safeguard is taken as failed. If both safeguards are in failed state upon a demand, then a hazard occurs.

    For parallel-detectable systems, the time between demands (or between the first demand and the previous test) is the same for both safeguards. For series-detectable systems, the secondary safeguard is not challenged as frequently as the primary safeguard. Therefore, these two safeguards usually have different time periods. For undetected systems, at each demand, a determination is made of the status of each of the safeguards. If either safeguard is determined to be in a failed state, then it remains in a failed state until either the next testing period or until the other safeguard also fails, resulting in the hazard.
(4) Sum the number of hazards for all demands in the test interval for the given number of demands to give the "expected" number of hazards, *N* for a given number of demands for that trial.
(5) Repeat steps 2–4 numerous of times to get a statistical sample and take the average value of expected number of hazards (*N*) for each given number of demands per test interval.
(6) For each number of demands in a test interval, multiply the expected number of hazards by the frequency of a demand in a test interval (determined from step 1), giving the hazard rate per number of demands per test interval.
(7) Sum together the values in step 6 for all the discrete number of demands, giving the hazard rate per test interval.
(8) Multiply the value in step 7 with the testing frequency, $1/T$ (tests per time period), giving the hazard rate.

4. Analysis

This analysis was carried out using an Excel spreadsheet. Fig. 2a–d gives the hazard rate from this analysis for a wide range of failure and demand rates for dual safeguard systems. These graphs show that parallel, detectable systems can produce a significantly lower hazard rate than series, detectable systems, with both trailed by undetected systems. For example, given a safeguard failure rate of 0.1 and a demand rate of 10 per test interval, a series-detectable and an undetected system have respective hazard rates 3 times and 4.5 times greater than a parallel-detected system. As described earlier, the safeguards in the parallel-detect arrangement are tested the most frequently, increasing their reliability. With the series arrangement, the primary safeguard is challenged relatively frequently, but the secondary safeguard is only challenged when the primary safeguard fails, or during one of the official tests. With the undetected safeguards, no knowledge is gained when they

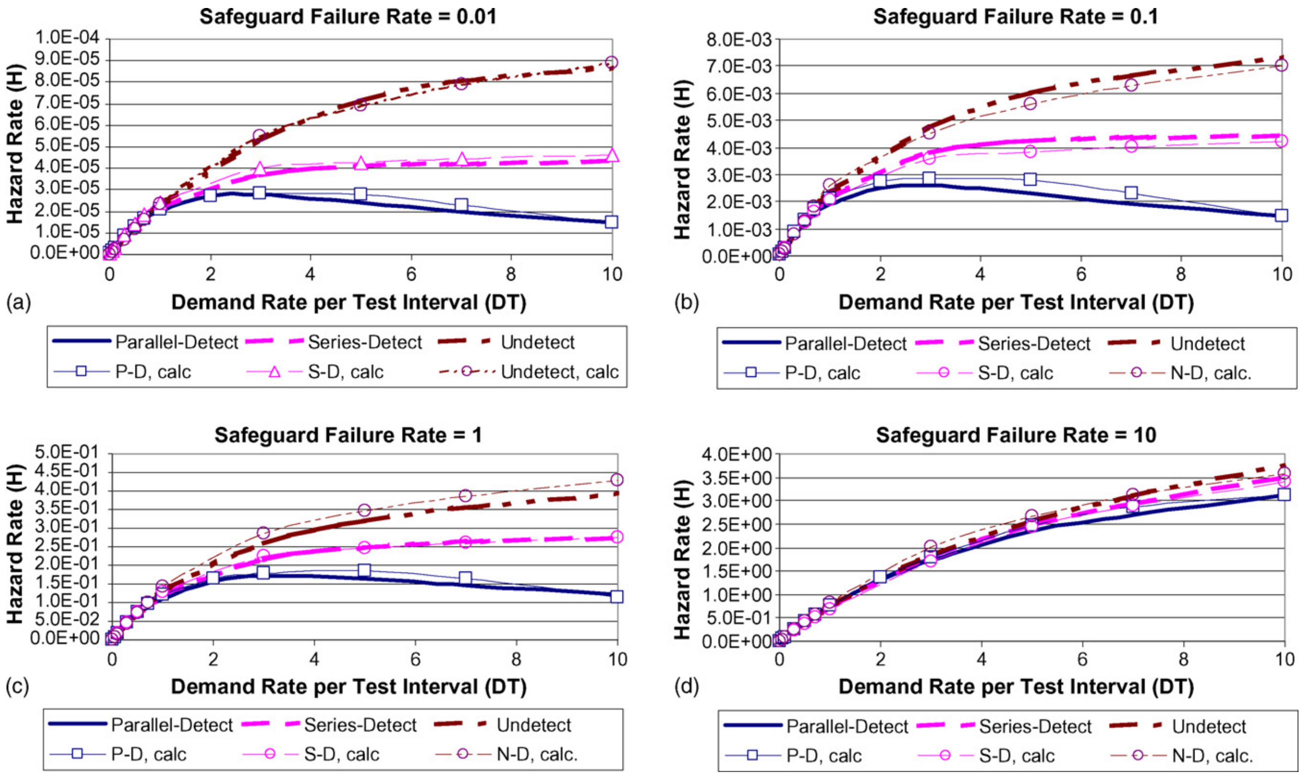

Fig. 2. Hazard rate comparison: (a) safeguard failure rate = 0.01; (b) safeguard failure rate = 0.1; (c) safeguard failure rate = 1; (d) safeguard failure rate = 10.

Table 1
Empirical hazard rate formulas for two safeguard systems

System	Validity range		Empirical hazard rate (H)
	DT	λT	
All	$DT[0.1$	$\lambda T[0.1$	$H = D(\lambda T)^2$ (analytical equation)
Parallel-detect	$2[DT[10$	$1 < \lambda T < 10$	$H = D\{0.2976 \ln(\lambda T) + 0.0741\}\, \mathrm{e}^{-\{0.0017(\lambda T)^2 - 0.0347(\lambda T) + 0.2685\}DT}$
		$0.1[\lambda T[1$	$H = D\{0.1211(\lambda T)^{1.7606}\}\, \mathrm{e}^{-\{0.0017(\lambda T)^2 - 0.0347(\lambda T) + 0.2685\}DT}$
		$\lambda T < 0.1$	$H = 0.21D(\lambda T)^2\, \mathrm{e}^{-0.265DT}$
	$DT < 2$	$1 < \lambda T < 10$	$H = D\{0.3079 \ln(\lambda T) + 0.1757\}\, \mathrm{e}^{-\{0.0032(\lambda T)^2 - 0.0637(\lambda T) + 0.4478\}DT}$
		$0.1[\lambda T[1$	$H = D\{0.1791(\lambda T)^{1.7346}\}\, \mathrm{e}^{-\{0.0032(\lambda T)^2 - 0.0637(\lambda T) + 0.4478\}DT}$
		$\lambda T < 0.1$	$H = 0.33D(\lambda T)^2\, \mathrm{e}^{-0.441DT}$
Series-detect	$3[DT[10$	$0.5 < \lambda T[10$	$H = (1/T)[\{0.1507(\lambda T) - 0.1107\} \ln(DT) + 0.0018(\lambda T)^3 - 0.0477(\lambda T)^2 + 0.3249(\lambda T) - 0.0974]$
		$0.01 < \lambda T[0.5$	$H = (1/T)[0.0493(\lambda T)^{1.988} \ln(DT) + 0.2688(\lambda T)^{1.9478}]$
	$0.01 < DT < 3$	$0.5[\lambda T[10$	$A = 1\mathrm{e}^{-4}(\lambda T)^3 - 0.002(\lambda T)^2 + 0.0112(\lambda T) - 0.0025$ $B = 7\mathrm{e}^{-4}(\lambda T)^3 - 0.0139(\lambda T)^2 + 0.0869(\lambda T) - 0.0212$ $C = 1.3\mathrm{e}^{-3}(\lambda T)^3 - 0.0327(\lambda T)^2 + 0.289(\lambda T) - 0.0826$ $H = (1/T)\{A(DT)^3 - B(DT)^2 + C(DT)\}$
		$0.01 < \lambda T < 0.5$	$H = (1/T)\{0.0088(\lambda T)^{1.8322}(DT)^3 - 0.0808(\lambda T)^{1.9275}(DT)^2 + 0.2484(\lambda T)(DT)\}$
Un-detected	$1 < DT[10$	$0.5 < \lambda T[10$	$H = (1/T)\{(-0.0037(\lambda T)^2 + 0.1711(\lambda T) - 0.0497) \ln(DT) + (3 \times 10^{-4}(\lambda T)^3 - 0.0142(\lambda T)^2 + 0.1715(\lambda T))\}$
		$0.01 < \lambda T[0.5$	$H = (1/T)\{0.1525(\lambda T)^{1.8642}\} \ln(DT) + \{0.2114(\lambda T)^{1.9775}\}$
	$0.01[DT[1$	$0.5 < \lambda T[10$	$H = D\{0.001(\lambda T)^3 - 0.0244(\lambda T)^2 + 0.2332(\lambda T) - 0.0677\}$
		$0.01 < \lambda T[0.5$	$H = (D/T)\{-0.1926(\lambda T)^3 + 0.2837(\lambda T)^2 - 5\mathrm{e}^{-4}(\lambda T)\}$

Note. Equations derived from Monte Carlo simulation.

are challenged, so they cannot be repaired when needed, except during the periodic tests.

It is interesting to note that at a low to moderate safeguard failure rates, the parallel-detect hazard curve reaches a peak around two demands per test interval, and then actually declines with increasing demands. Apparently the advantage of detecting safeguard failures during operation outweighs the risk of both safeguards being in a failed state at the same time during a demand. At a relatively high failure rate (10 per test interval), it seems that the likelihood of both safeguards being out of service when needed is sufficiently high that there is reduced value in being able to detect safeguard failures. Note that all three systems converge at low demand rates. At low demand rates, the ability to detect failures during operation becomes less significant when compared to the periodic safeguard tests. Simplified Eq. (5) can be applied when the demand rate and testing rate are low (<0.1 per test interval).

Empirical equations were developed from this Monte Carlo simulation, given in Table 1. These equations were plotted as shown in Fig. 2, showing a good fit with the Monte Carlo simulation over the given range of safeguard failures and demand rates.

Finally, one of the conditions was that each of the safeguards in a system is tested on the same schedule. This actually gives the highest hazard rate since both safeguards approach their most vulnerable period at the same time. Instead, consider staggering the testing schedules. For example, if the demand and failure rate (per test interval) are small, then if the two safeguards are tested at half periods from each other, the hazard rate would be as follows:

$$H = \frac{D \times 2}{T} \int_0^{T/2} (\lambda_a t)(0.5\lambda_b T + \lambda_b t)\,dt = \frac{D[5\lambda_a\lambda_b T^2]}{24} \qquad (6)$$

Comparing this equation with Eq. (5) shows that simply by staggering the testing schedules, the hazard rate can be reduced by 38%.

5. Summary

The hazard rate for two safeguard systems can be solved analytically given a low demand and low safeguard failure rate. A Monte Carlo simulation was used to find general solutions for these systems. Empirical formulas for two safeguard systems were derived from this analysis and are given for the various configurations of two safeguard systems.

On a qualitative basis, two safeguards are obviously better than one. However, the arrangement of these safeguards can significantly affect the overall hazard rate. When the demand rate is low, it does not make much difference how the safeguards are configured. Otherwise, it is best to install the safeguards to both actuate on the same demand and provide positive feedback to indicate whether they functioned correctly. The safeguards can also be configured to actuate at different time steps, but with reduced effectiveness. The lowest reliability is given when the safeguards do not provide positive feedback to indicate their operational status, upon demand. Regardless of which configuration is selected, the hazard rate can be minimized by staggering the testing schedules of the safeguards.

References

[1] M.J. Rothschild, Updated hazard rate equation for single safeguards, J. Hazard. Mater. 130 (1–2) (2006) 15–20.

[2] F.P. Lees, Loss Prevention in the Process Industries, vol. 1, 3rd ed., Elsevier/Butterworth/Heinemann, Oxford, England, 2005, pp. 7/28–7/32.

Glossary

Expected number of hazards (N): The expected number of hazards in a test interval.

Hazard: An undesired event that can result in undesired safety, environmental or financial consequences. Hazards are deviations from normal operations and require the occurrence of an initiating cause with the failure of the safeguard.

Hazard rate (H): The frequency (occasions per time period) at which a hazard is expected to occur. For example, the frequency at which the pressure in a vessel exceeds the design pressure or the frequency at which a vessel is overfilled. The hazard rate can range from a rare calculated event to a frequent event where the rate can be measured.

Initiating cause: An undesired cause of deviation from normal operation parameters that can lead to a hazard. Examples of initiating causes include a stuck control valve, a pump failure, and failure to follow procedures.

Safeguard: One or more components installed as a unit to prevent the hazard from occurring, either by reducing the likelihood of the initiating cause or by mitigating the consequences of the hazard. For this definition, components can be equipment (rupture disk, level gauge, etc.) or administrative (procedures, personal protective equipment, etc.).

Safeguard failure rate (λ): The average frequency that a safeguard is estimated to fail.

Safeguard in a failed state upon demand (Q): The conditional likelihood that a safeguard would fail, upon demand.

System demand rate (D): The frequency (occasions per time period), on average, at which an initiating cause occurs. The rate can be measured, if frequent, or estimated if not.

Testing interval (T): Time period between independent tests of the safeguards. A year is a typical test interval, but test intervals can range from essentially continuous to no tests at all.