ELSEVIER

Journal of Hazardous Materials 130 (2006) 15–20

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

Updated hazard rate equation for single safeguards

Marc Rothschild [*]

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

Available online 16 September 2005

Abstract

Commonly used equations have been developed which allow application of failure rate data for safeguards. While these equations often give reasonable results, they can significantly over predict the risk for some conditions. This can lead the analyst to believe that a given operation presents an unacceptable risk, requiring additional safety measures when, in fact, the operation may actually meet the risk criteria. This paper shows the limitations of the commonly used equations by comparing those equations with hazard rates generated from Monte Carlo simulations. A little-known equation is then presented, which is shown to precisely match the Monte Carlo simulations. It is suggested that this equation be used when accuracy is required.

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

1. Introduction

Hazards can occur when a demand is placed on a system that can lead to an adverse consequence and the safeguards 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 safeguards fail upon demand:

$$\text{hazard rate (HR)} = \text{demand rate } (D) \times \text{safeguard failure upon demand } (Q) \tag{1}$$

This equation forms the basis of the Layer of Protection Analysis (LOPA). The analysis is trivial if the demand rate and the conditional probability of failure of the safeguards are known. However, while the demand rate is usually known or can be reasonably estimated, the safeguard failure data is often given in the literature as a failure rate instead of as a conditional failure probability. In those cases, in order to apply Eq. (1), the given safeguard failure rate must first be converted to a failure-upon-demand basis.

This paper presents two commonly used equations for evaluating the hazard rate given the safeguard failure rate. These equations are compared against hazard rate data curves that were generated from Monte Carlo simulation, showing their respective limitations. Another equation is then presented that is shown to accurately match the Monte Carlo simulations, and is thus presented as the most accurate hazard rate equation. The basis for all of the approaches presented in this paper are as follows:[1]

- the systems under consideration are protected by a single safeguard;[2]
- the safeguard is tested at regular defined intervals;
- failures and demands are random;
- 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).

[*] Tel.: +1 215 785 7327; fax: +1 215 785 7077.
E-mail address: mrothschild@rohmhaas.com.

[1] While the basis for this analysis applies to many situations, it is not universal. None of the given equations in this paper apply unless all of these conditions are met.

[2] Additional complications are sometimes introduced when more than one safeguard is applied, invalidating these formulas.

0304-3894/$ – see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2005.07.036

2. Safeguard failure analysis

2.1. Simplified straight-line equation

As stated above, hazards can occur when a demand is placed on a system that can lead to an adverse consequence and the safeguard to prevent the consequence is in a failed state. The probability of system failure prior to time (t) is given by the cumulative distribution function $Q(t)$. This function is derived by applying the Poisson distribution to the component failure rate (λ):

$$Q(t) = 1 - \mathrm{e}^{-\lambda t} \tag{2}$$

The cumulative likelihood of a safeguard being in a failed state increases with time until the safeguard is tested, and subsequently repaired, if needed. Therefore, the likelihood of a safeguard being in a failed state at any given time (also known as the safeguard unavailability) ranges from zero (right after testing) to $1 - \mathrm{e}^{\lambda T}$ (right before the next test at time "T"). Since demands are random, if there is only the potential for a single demand in a test interval, this demand could occur at any time in the test interval. The hazard rate can be determined by integrating the demand rate multiplied by the conditional probability of safeguard failure over the test interval:

$$\mathrm{HR} = \frac{1}{T}\int_0^T D(1 - \mathrm{e}^{-\lambda t})\mathrm{d}t \tag{3}$$

When $\lambda t \ll 1$, then the term $(1 - \mathrm{e}^{-\lambda t})$ in Eq. (2) simplifies to

$$Q(t) = \lambda t \quad (\text{when}\, \lambda t \ll 1) \tag{4}$$

The hazard rate in Eq. (3) then simplifies to:

$$\mathrm{HR} = \frac{D}{T}\int_0^T \lambda t\, \mathrm{d}t \tag{5}$$

Solving Eq. (5) gives:

$$\mathrm{HR} = \frac{D\lambda t}{2} \tag{6}$$

Eq. (6) is a commonly used, straight-line equation for evaluating the hazard rate when the safeguard failure data is given as a failure rate. This equation has enjoyed widespread use, as it is simple to use and is sufficiently accurate in most applications. However, as discussed below, it is not valid for large failure rates and large demand rates.

As derived above, the simplified straight-line equation is based on a highly reliable safeguard ($\lambda T \ll 1$). When this basis is not valid, then the actual hazard rate, as determined from Eq. (3) is less than the straight-line approximation given in Eq. (6). Furthermore, this equation only applies to the potential for a single demand in a test interval. If there were multiple demands in a test interval, then the likelihood of failure immediately following each demand would be zero, as the safeguard would either be found to be working or it would be subsequently repaired. In this regard, demands are in some respects the same as tests, as they both evaluate the condition of the safeguard, with the obvious difference that, given a failed safeguard, a demand results in a hazard, whereas detecting a failed safeguard during a test is benign. The time period between demands decreases with increasing number of demands, resulting in decreased safeguard unavailability at each demand. In contrast, Eq. (6) treats the conditional probability of safeguard failure ($\lambda T/2$) as independent of the demand rate. Therefore, the equation over predicts the hazard rate for high demand situations, as shown in Fig. 1. It should be intuitive that the hazard rate cannot exceed the safeguard failure rate and that this equation cannot apply above the dashed line in Fig. 1.

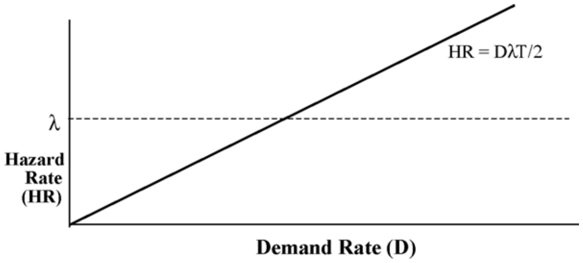

Fig. 1. Straight-line simplification.

2.2. High/low demand equation

To prevent the hazard rate from exceeding the safeguard failure rate, Eq. (6) has been modified into two straight-lines, as given by Eq. (7) and as shown in Fig. 2. This modification to the straight-line equation is referred to as the high/low demand equation [1–4]. This equation prevents the hazard rate from exceeding the safeguard failure rate. At very high demand rates, it is apparent that the true hazard rate approaches the safeguard failure rate as given in this approach (that is, if there are a large number of demands in a test interval, then if the safeguard were to fail, there almost certainly would be a demand following the safeguard failure). This approach provides a conservative upper estimate for moderate demand rates and for moderate to high safeguard failure rates, which may be suitable for many applications. However,

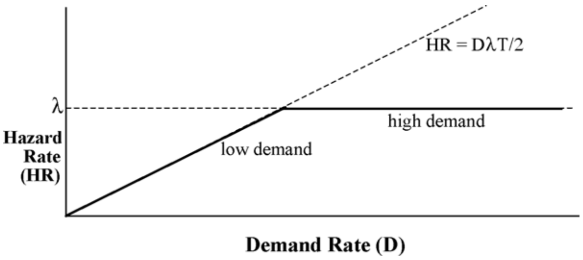

Fig. 2. High/low demand straight-line modification.

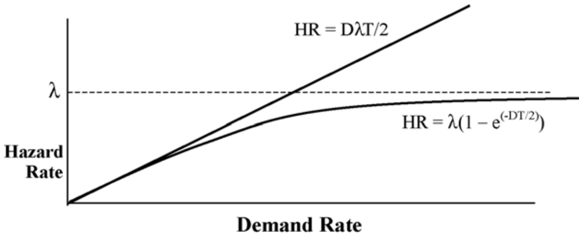

Fig. 3. Approximate analytical solution.

sometimes a more accurate analysis is needed.

$$\mathrm{HR} = \mathrm{MAX}\left(\frac{D\lambda T}{2}, \lambda\right) \tag{7}$$

2.3. "More accurate" equation

Dr. Trevor Kletz introduced the following equation as a "more accurate" equation [5] and draft ISA-TR.84.00.04 [4] refers to it as "rigorous":

$$\mathrm{HR} = \lambda \cdot (1 - \mathrm{e}^{-DT/2}) \tag{8}$$

This equation, shown in Fig. 3, matches up with the straight-line equation for low demand rates, approaches the safeguard failure rate for high demand rates, and does not have any unexpected discontinuity, as shown in the high/low demand equation. Visually, this relationship appears to be accurate; however, dissection of this equation reveals its limitations.

As stated in the basis, a failure can occur randomly across a test interval with uniform probability. The tacit assumption is made in Eq. (8) that the failure occurs at the midpoint of the test interval. It follows then that given an average of *DT* demands in a given test interval, the expected number of demands *after* the failure is *DT*/2. Based on Poisson's law, the likelihood of a demand occurring after the midpoint is:

$$\Omega = 1 - \mathrm{e}^{-DT/2} \tag{9}$$

The derivation of Eq. (8) is completed by multiplying the failure rate (λ) with the conditional probability of a demand following the safeguard failure ($\Omega = 1 - \mathrm{e}^{-DT/2}$).

There are two simplifications made in Eq. (8), both resulting in over prediction of the hazard rate. The first simplification is in tacitly locating the failure at the midpoint of the test interval range. The actual distribution of the failure of the safeguard is random, and is therefore linear across the test interval. Based on Poisson's law, the likelihood of a demand occurring after any point in time is:

$$\Omega = 1 - \mathrm{e}^{-DT} \tag{10}$$

Thus, the actual expected hazard rate is determined by integration to be:

$$\mathrm{HR} = \lambda \frac{\int_0^T (1 - \mathrm{e}^{-Dt})\mathrm{d}t}{T} \tag{11}$$

Solving this equation shows that the average hazard rate is less than the value taken at the midpoint, so that selecting the midpoint value is overly conservative. As a special application, when $Dt \ll 1$, Eq. (11) simplifies to the straight-line equation as given in Eq. (6):

$$\mathrm{HR} = \lambda \left[\frac{\int_0^T Dt\,\mathrm{d}t}{T}\right] = \frac{\lambda DT}{2}$$

Another simplification is that Eq. (8) is based on the assumption that the safeguard failure rate is an independent parameter (i.e., hazard rate is directly proportional to the failure rate). This is true for an initial failure, which is taken as a random event. However, a second failure within a test interval *cannot* occur until there is first a system demand *following* the initial failure. Likewise, a third failure cannot occur until there is a second demand, and so on. For multiple failures within a test interval, the failure rate *is* dependent on the occurrence and timing of demands. Thus, for high failure rate safeguards, Eq. (8) will overestimate the actual hazard rate.

2.4. Comparing high/low demand and "more accurate" equations with actual hazard rate

Solving for the hazard rate, given demand and failure frequencies, involves converting the failure rate to a conditional probability of failure as a function of time as given in Eq. (2):

$$Q(t) = 1 - \mathrm{e}^{-\lambda t}$$

The likelihood of the safeguard being in a failed state at the next demand is solved by applying the time (*t*) between the current demand, and the previous demand or test to the above equation. This likelihood is then multiplied by the frequency of the demand to give the hazard rate. The hazard rate is solved using a Monte Carlo simulation, where the placement of the demands are randomly made and repeated multiple times to give a representative sampling. The approach taken, depicted in Fig. 4, is as follows:

(1) From the average demand-rate-per-test interval, determine the distribution and frequency of the discrete possible number of demands in a given test interval, based on a Poisson distribution.
(2) For each select number of demands-per-test interval, randomly distribute the demands in the test interval by applying the Poisson distribution.
(3) Evaluate the conditional probability of failure at each demand ($Q = 1 - \mathrm{e}^{-\lambda \Delta t}$).
(4) Sum the conditional probability of failures for all demands in the test interval for a given number of demands to give the "expected" number of failures, *N*.
(5) Repeat Steps 2–4 thousands of times to get a representative sample and take the average value for the number of failures per demand-per-test interval.
(6) For each number of demands in a test interval, multiply the value from Step 5 by the frequency of a demand in a

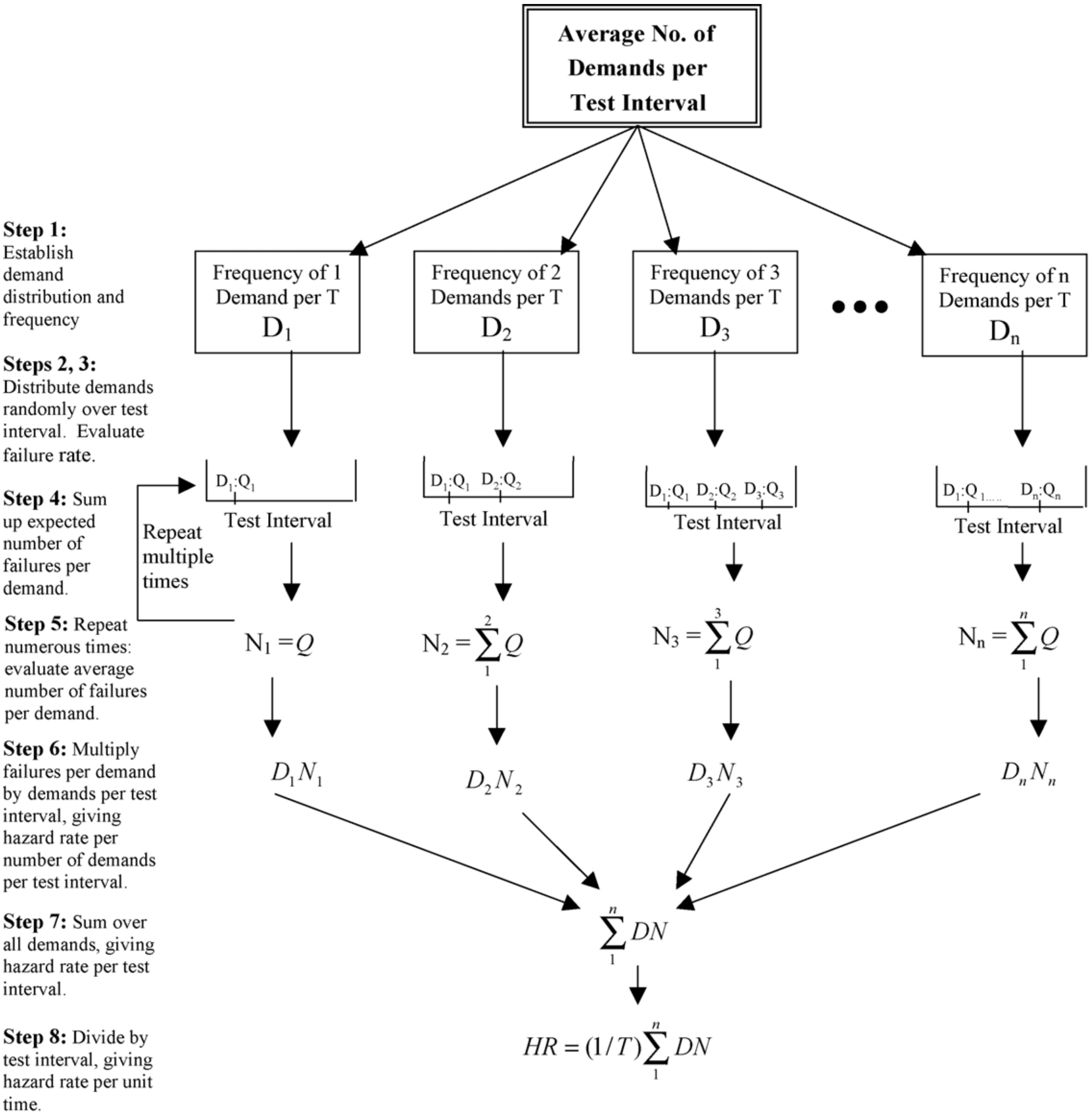
Average No. of Demands per Test Interval
Step 1: Establish demand distribution and frequency
Frequency of 1 Demand per T D1
Frequency of 2 Demands per T D2
Frequency of 3 Demands per T D3
Frequency of n Demands per T Dn
Steps 2, 3: Distribute demands randomly over test interval. Evaluate failure rate.
D1:Q1
D1:Q1 D2:Q2
D1:Q1 D2:Q2 D3:Q3
D1:Q1 ..... Dn:Qn
Test Interval
Step 4: Sum up expected number of failures per demand.
Repeat multiple times
Step 5: Repeat numerous times: evaluate average number of failures per demand.
N1 = Q
N2 = Σ Q
N3 = Σ Q
Nn = Σ Q
Step 6: Multiply failures per demand by demands per test interval, giving hazard rate per number of demands per test interval.
D1N1
D2N2
D3N3
DnNn
Step 7: Sum over all demands, giving hazard rate per test interval.
Σ DN
Step 8: Divide by test interval, giving hazard rate per unit time.
HR = (1/T) Σ DN

Fig. 4. Flow chart for evaluating hazard rate.

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.

Fig. 5 gives a comparison of the hazard rate as evaluated by this rigorous approach with that given by the high/low demand Eq. (7) and the "more accurate" Eq. (8). These figures show that both of these equations are valid for small values of λT and DT.[3] However, both Eqs. (7) and (8) over predict the hazard rate for all larger values of λT and DT. This over prediction can range from approximately 15% for small failure rates to several 100% for larger failure rates.

2.5. "Most accurate" equation

A confidential source provided the following hazard rate equation, given as Eq. (12). As shown in Fig. 5, this equation perfectly matches the Monte Carlo simulation for all tested ranges of failure and demand rates, and is therefore presented as the "most accurate" hazard rate equation.

$$\text{Hazard rate} = \left[D\frac{\lambda}{D+\lambda}\right]\times\left\{1-\frac{(1-\mathrm{e}^{-(D+\lambda)T})}{(D+\lambda)T}\right\} \qquad (12)$$

[3] From a practical perspective, these equations are valid when λT and DT are less than 0.1.

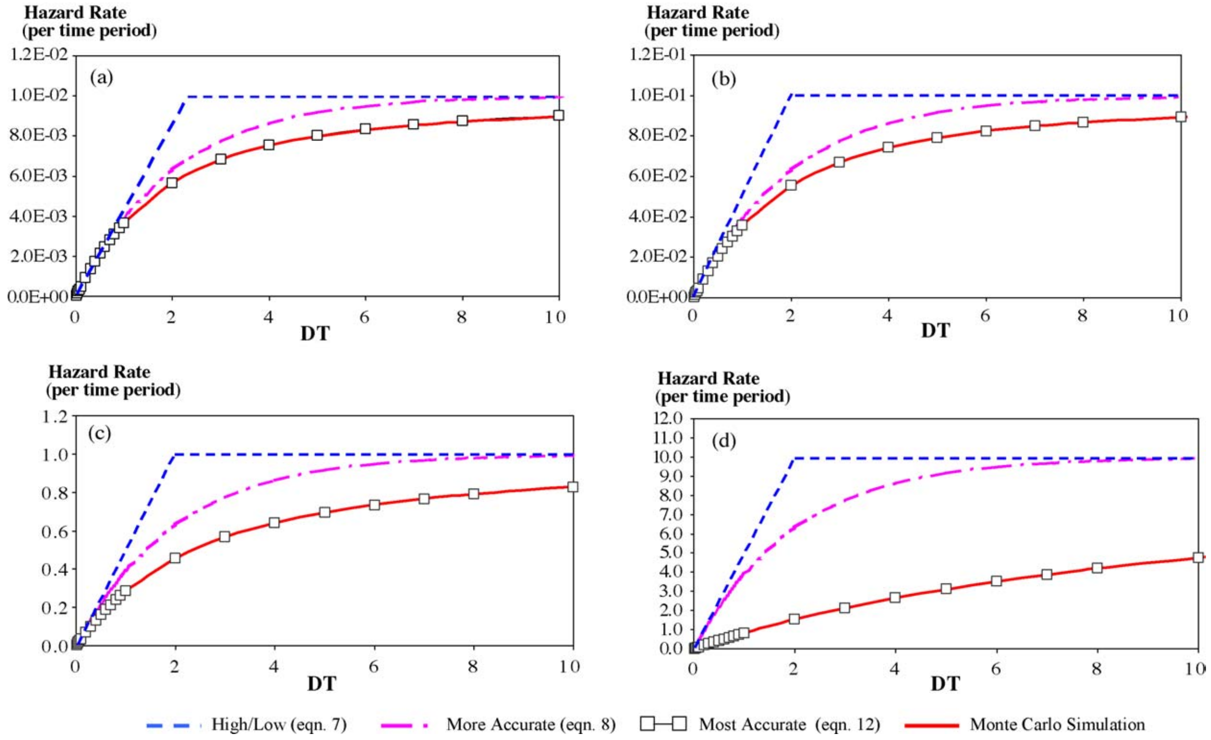

Fig. 5. Hazard rate comparison. (a) Safeguard failure rate = 0.01 per test interval. (b) Safeguard failure rate = 0.1 per test interval. (c) Safeguard failure rate = 1 per test interval. (d) Safeguard failure rate = 10 per test interval.

Table 1
Comparison of failure rate equations

Failure rate per test period	Demand rate per test period	Straight-line (Eq. (6))	High/low demand (Eq. (7))	"More accurate" (Eq. (8))	"Most accurate" (Eq. (12))
Low (<0.1)	Low (<0.1)	Excellent	Excellent	Excellent	Excellent
	Moderate (1)	Fair	Fair	Good	Excellent
	High (10)	Poor	Good	Good	Excellent
Moderate (1)	Low (<0.1)	Good	Good	Good	Excellent
	Moderate (1)	Fair	Fair	Good	Excellent
	High (10)	Poor	Good	Good	Excellent
High (10)	All	Poor	Poor	Fair	Excellent

3. Conclusion

Table 1 presents a comparison of these failure rate equations. This table shows that the simplified straight-line Eq. (6) is suitable when the safeguard failure rate and the system demand rate are low, which is commonly the case. However, this equation overestimates the failure rate for moderate demand rates and is unsuitable for use for high demand rates. The high/low demand Eq. (7) likewise overestimates the risk at moderate demand rates, but may be reasonable for high demand rates. The "more accurate" Eq. (8) presents an improvement over the straight-line approach for moderate demand rates, but still overestimates the actual failure rate. None of these equations are suitable given a high safeguard failure rate. Only Eq. (12) accurately gives the hazard rate for the wide range of evaluated failure and demand rates. The "most accurate" Eq. (12) should be used when either the failure rate or the demand rate is not low and accuracy is required.

Appendix A

Definitions[4]

Demand following failure (Ω) The conditional likelihood that a demand occurs following a failure of a safeguard. A hazard only occurs if a demand follows a safeguard failure

[4] It is recognized that there is considerable variation in terminology and definitions in the field of risk analysis. This table is intended to help readers understand how the terms are used in this paper.

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

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 (HR) 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, PPE, etc.)

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

Safeguard failure-upon-demand (Q) The conditional likelihood that a safeguard would fail, upon demand

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

References

[1] IEC, IEC 61511, Functional Safety Instrumented Systems for the Process Industry Sector, Parts 1–3, International Electrotechnical Commission, Geneva, 2001.

[2] IEC, IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, Parts 1–7, International Electrotechnical Commission, Geneva, 1998.

[3] Center for Chemical Process Safety (CCPS), Layer of Protection Analysis, Simplified Process Risk Assessment, New York American Institute of Chemical Engineers, 2001.

[4] ISA, ISA-TR84.00.04 Part 1, Guideline on the Implementation of ANSI/ISA 84.00.01-2004 (IEC 61511 Mod), Annex I Continuous Mode Versus Demand Mode, Instrument Society of America, Research Triangle Park, NC, 2004.

[5] T.A. Kletz, HAZOP & HAZAN, Notes on the Identification and Assessment of Hazards, The Institution of Chemical Engineers, Rugby, UK, 1983.