Energy, Mines and Resources Canada | Énergie, Mines et Ressources Canada

CANADA CENTRE FOR MINERAL AND ENERGY TECHNOLOGY
(Former Mines Branch)

RISK ANALYSIS APPLIED TO FLAMEPROOFING OF DIESEL EXHAUST SYSTEMS

PRELIMINARY PHASE

P. MOGAN, W.M. GRAY AND D.B. STEWART

ENERGY RESEARCH LABORATORIES
MINING RESEARCH LABORATORIES

MAY 1975

For presentation at the 16th International Conference of Coal Mine Safety Research, Washington, D.C., September 22-26, 1975

ENERGY RESEARCH LABORATORIES
REPORT ERP/ERL 75-68 (OP)

RISK ANALYSIS APPLIED TO FLAMEPROOFING OF DIESEL EXHAUST SYSTEMS PRELIMINARY PHASE

P. Mogan, W.M. Gray and D.B. Stewart

Canada Centre for Mineral and Energy Technology
Department of Energy, Mines and Resources
Ottawa, Ontario, Canada

INTRODUCTION

It has been shown recently by de Heer (1) of the Dutch State Mines that the probability of a dangerous event resulting from a given hazard can be calculated from an estimate of the mean frequency of occurrence of the hazard together with a knowledge of the failure rate of the associated protective devices and the frequency at which they are inspected, with consequent correction of any failure.

Calculations by de Heer yield the level of safety associated with a given safety system in terms of the mean time before failure (MTBF), signifying the dangerous coincidence of a safety system failure with a hazardous process upset. Recognizing that failure of the safety exhaust system of a diesel mining machine in a flammable mine atmosphere could lead to anything from a localized inflammation of the mine air to a catastrophic mine explosion, we will use the term MTBE, signifying Mean Time Before a Dangerous Event, to cover the full range of possibilities, and to allow the term "failure" to be reserved for the description of the non-operational state of a safety device.

MTBF's are derived by de Heer for various types of protective systems in terms of λ , μ and τ_0 where:

λ is the mean frequency of occurrence of a hazard,

μ is the mean frequency of the 'open-mode' * failures of the safety device, and

τ_0 is the time duration of the 'open-mode' failure of the safety device.

His formulae are based on process-plant upsets, in which the identical parallel safety components are assumed to be quite reliable, $\mu_1 = \mu_2 = \mu_3 = 0.02$, and the hazardous upsets fairly frequent, $\lambda = 2$. This situation

* 'open-mode' failure occurs when the safety device fails to act during a hazardous condition, as distinct from a 'short-mode' failure in which a safety device initiates an unnecessary shutdown when no hazard is present.

is reversed in the case of safety systems used on the exhaust of a flameproof diesel mining vehicle, where the hazardous process upset considered here (an exhaust backfire) is infrequent, while frequent failure of the safety devices could be expected due to the severe working environment.

Formulae to reflect the latter case are derived in the Appendix. The derivation is straightforward, does not require approximations that would be inaccurate for safety systems subject to frequent failure (μ not $\ll 1$), and includes the possibility of systems with widely divergent characteristics ($\mu_1 \neq \mu_2 \neq \mu_3$, $\tau_{01} \neq \tau_{02} \neq \tau_{03}$) The formula derived for a doubly redundant system is:

$$\text{MTBE} = \frac{1}{\lambda\, \tau_{01} \tau_{02} \tau_{03} (1 - e^{-\mu_1})(1 - e^{-\mu_2})(1 - e^{-\mu_3})}$$

where the subscripts 1, 2 and 3 refer respectively to the three safety devices.

FLAMEPROOF DIESEL MINING VEHICLE EXHAUST SYSTEMS

For a flameproof diesel mining vehicle, the event for which protection is provided is the propagation of an exhaust backfire into a flammable mine atmosphere. The protective devices include a water-filled scrubber and a plate-type exhaust flametrap. Water depletion in the scrubber to an unsafe level is prevented by low-water shutdown and high-temperature shutdown devices. Failure of the safety devices can be assumed to be discovered and corrected at various intervals, such as the start of each day shift, during routine vehicle maintenance or during periodic inspection by regulatory authorities.

Evaluation of Parameters

Little data is available to estimate the frequency of diesel engine backfire in mining service, or the frequency of safety system failure. MTBE's calculated from hypothetical data, however, provide a means of comparing the relative levels of protection for various safety systems. Substitution of alternate values from the reader's experience can provide a yardstick to measure against de Heer's criterion for an adequately protected process - one in which the expectancy of calamity does not significantly reduce the life expectancy of a 20-to 30-year-old worker.

λ - Backfire Frequency

For an exhaust backfire to precipitate a dangerous event, a flammable mine atmosphere must be present simultaneously. In the case in which the frequency of one component of a hazard is radically different from another, the rate of occurrence dictated by the less frequent component

will determine the level of safety, with the more frequent assumed to be more or less continuously present. This type of reasoning is used by Benjaminsen and van Weichen (2) to conclude that U.K. Division 0 and U.K. Division 1 locations for flameproof electrical equipment represent an equivalent probability of hazard - i.e. the low incidence of failure of the protective device renders the distinction between continuous and likely exposure insignificant. On this basis, a flammable mine atmosphere will be assumed to be continuously present, so that λ will be wholly derived from the frequency of backfire.

An engine manufacturer has provided data from a two year reliability analysis study suggesting that 0.04% of an engine group exhibited defects which could lead to backfiring during a two year period. Since many of these engines would be used for road transport or construction, a utilization factor of X2 could be included for three shift mining operation. The yearly frequency of such defects in mining service would then be $\frac{0.04}{100} \times \frac{2}{2} = 0.0004$. All of the defects would not necessarily produce a backfire but, as those that would could produce several before the mechanical malfunction was corrected, the frequency of backfire λ will be assumed to also equal 0.0004 per year.

μ - 'Open-mode' Failure Rate of the Safety Devices

Normal mechanical failure of the low-water shutdown and high-temperature shutdown devices is arbitrarily assumed to occur twice per year. As these devices are normally independent, they function as a redundant safety system, and $\mu_1 = \mu_2 = 2$.

During start-up, however, due to thermal lag, the high-temperature device will not shut the engine off immediately even though the scrubber is empty. The safety system will then be non-redundant at start-up, with $\mu_1 = 2$.

A similar situation may occur if the scrubber water is depleted in a remote section of the mine. In this circumstance there may be a tendency for the operator to defeat both devices to avoid taking the machine out of service until water to fill the scrubber can be obtained more conveniently. Such a simultaneous 'failure' of both devices must be considered as the failure of a single device, as they are not allowed to function in their normally independent modes. It is arbitrarily assumed that this type of failure will also occur twice per year with $\mu_{12}^* = 2$

* μ_{12} signifies a deliberate coincidence of μ_1 with μ_2

Failure of a plate-type flame arrester could result from improper assembly or fitting. If the arrester must be cleaned each day the rate of occurrence of improper fitting could be fairly great, say once every 125 shifts or six times per year, so that $\mu_3 = 6$ per year. (cases II, VI). However, failure could also result from damage which we can arbitrarily assign a rate similar to the other safety device failures, $\mu_3 = 2$. (cases I, V).

τ_0 - Inoperative Periods of the Protective Devices

The mean duration of the failed state of the protective devices depends principally on the frequency of effective inspection and corrective maintenance. The effects of the following basic inspection practices are investigated.

If the protective devices are inspected each day, i.e. at the beginning of the day shift, the mean inoperative period will be 1/2 day, or 1.4×10^{-3} year, i.e. $\tau_{01} = \tau_{02} = \tau_{03} = 1.4 \times 10^{-3}$ year (except in the case of an improperly fitted plate-type flame arrester, for which the duration of the failed state will necessarily equal the cleaning interval, assumed to be one day or $\tau_{03} = 2.7 \times 10^{-3}$ year.)

Inspection during routine maintenance is assumed to be at five-week intervals. The mean inoperative period would then be 5/2 weeks = $5/2 \times 1/50 = 0.05$ year, i.e. $\tau_{01} = \tau_{02} = \tau_{03} = 0.05$ year.

Inspection by a regulatory authority, assumed to be at three-month intervals, yields a mean inoperative period of 3/2 months = $3/2 \times 1/12 = 0.125$ year, i.e. $\tau_{01} = \tau_{02} = \tau_{03} = 0.125$ year.

CALCULATION OF THE MTBE FOR SEVERAL HYPOTHETICAL CASES

The MTBE's calculated for several hypothetical circumstances, combining some or all of the protective devices and inspection frequencies, are summarized in Table I. In all of the cases, the frequency of occurrence of the hazard is assumed to be the same, i.e. $\lambda = 0.0004$ per year.

While numerous other combinations of circumstances could be envisaged, the following cases span the range of possibilities. They serve to illustrate the relative impact of the various factors, and indicate the type of data needed to provide a factual basis for assessing the adequacy of safety requirements.

Cases I A through II C

For these six cases, the diesel vehicle exhaust system is protected with the full complement of safety devices: a water-filled scrubber with low-water and high-temperature shutdowns, and a plate-type flame arrester. I A to I C assume failure of each safety device through random malfunction twice per year. The effect of increasing the mean time-to-repair from one half shift to one and one half months shows the expected decrease in MTBE. Cases II A through II C are similar to I A through I C, except that the plate-type flame arrester, rather than failing through random damage, is assumed to 'fail' through improper refit. As the flame arrester is cleaned and re-fitted daily, the maximum duration of this type of failure is necessarily only one day. Comparison of II A with I A shows, as expected, that the MTBE is reduced when the failure rate of the plate-type flame arrester is increased. But comparison of II B with I B, and II C with I C shows how the effect of the increased failure rate is offset by the effect of daily inspection, so that MTBE's are increased.

Cases III A through III C

These calculations represent a vehicle equipped with a wet scrubber and two shut-down devices only. Comparison with I A through I C illustrates the relative effectiveness of a doubly-redundant and a singly-redundant safety system.

Cases IV A through IV C

Here, the vehicle is equipped as in III, but it is assumed that only one shutdown device functions - as will occur at start-up, or in the case of deliberate pre-emption of the shut-down function (non-independent devices).

Case V A through VI C

These examples assess the effect of adding a plate-type flame arrester to the vehicle which is protected by a non-redundant water scrubber system as in case IV. Considerable increase in comparable MTBE's is observed, particularily in Case VI ('failure' due to improper refit) which represents the more likely 'failure' mode and duration for the plate-type flame arrester component.

TABLE 1

MTBE's for Various Combinations of Exhaust Safety Components and Inspection Frequencies

Backfire frequency λ = 0.0004/year for all cases

Case	Safety component used			Safety component failure rate $\frac{1}{\text{years}}$			Mean duration of failed state τ_0 years			MTBE for one vehicle, years	$\frac{\text{MTBE}}{10}$ years
	Low water shutdown # 1	High temperature shutdown # 2	Plate-type flame arrester # 3	μ_1	μ_2	μ_3	τ_{01}	τ_{02}	τ_{03}		
I A	✓	✓	✓	2	2	2	1.4×10^{-3}	1.4×10^{-3}	1.4×10^{-3}	1.41×10^{12}	1.41×10^{11}
I B	✓	✓	✓	2	2	2	0.05	0.05	0.05	3.09×10^{7}	3.09×10^{6}
I C	✓	✓	✓	2	2	2	0.125	0.125	0.125	1.98×10^{6}	1.98×10^{5}
II A	✓	✓	✓	2	2	6	1.4×10^{-3}	1.4×10^{-3}	2.7×10^{-3}	6.33×10^{11}	6.33×10^{10}
II B	✓	✓	✓	2	2	6	0.05	0.05	2.7×10^{-3}	4.97×10^{8}	4.97×10^{7}
II C	✓	✓	✓	2	2	6	0.125	0.125	2.7×10^{-3}	7.95×10^{7}	7.95×10^{6}
III A	✓	✓		2	2		1.4×10^{-3}	1.4×10^{-3}		1.71×10^{9}	1.71×10^{8}
III B	✓	✓		2	2		0.05	0.05		1.34×10^{6}	1.34×10^{5}
III C	✓	✓		2	2		0.125	0.125		2.14×10^{5}	2.14×10^{4}
IV A	✓	✓		μ_1^* or $\mu_{12}^{**} = 2$			τ_{01}^* or $\tau_{012}^{**} = 1.4 \times 10^{-3}$			2.06×10^{6}	2.06×10^{5}
IV B	✓	✓		" $= 2$			" $= 0.05$			5.78×10^{4}	5.78×10^{3}
IV C	✓	✓		" $= 2$			" $= 0.125$			2.31×10^{4}	2.31×10^{3}
V A	✓	✓	✓	" $= 2$		2	" $= 1.4 \times 10^{-3}$		1.4×10^{-3}	1.71×10^{9}	1.71×10^{8}
V B	✓	✓	✓	" $= 2$		2	" $= 0.05$		0.05	1.34×10^{5}	1.34×10^{5}
V C	✓	✓	✓	" $= 2$		2	" $= 0.125$		0.125	2.14×10^{5}	2.14×10^{4}
VI A	✓	✓	✓	" $= 2$		6	" $= 1.4 \times 10^{-3}$		2.7×10^{-3}	7.67×10^{8}	7.67×10^{7}
VI B	✓	✓	✓	" $= 2$		6	" $= 0.05$		2.7×10^{-3}	2.15×10^{7}	2.15×10^{6}
VI C	✓	✓	✓	" $= 2$		6	" $= 0.125$		2.7×10^{-3}	8.59×10^{6}	8.59×10^{5}

* Start-up μ_2 non functional due to thermal lag

** Pre-emption μ_1 and μ_2 do not act independently

Each of the preceding cases considers only a single diesel mining vehicle. An operating mine normally has several flameproof vehicles, with the probability of malfunction of one unrelated to the malfunction of another. The consequence of malfunction, however, could involve the environment of all of the vehicles if an explosion of the general mine atmosphere were precipitated. Therefore, increasing the number of vehicles could reduce the MTBE by an order of magnitude, as illustrated by the final column of Table 1.

CONCLUSIONS

It has been shown that the type of risk analysis proposed by de Heer (1) can be applied to the risk of explosion caused by exhaust backfire from diesel engines used in gassy underground mines. While the data presented is entirely hypothetical, the analysis does define the periods of maximum hazard such as start-up and pre-emption of the scrubber safety shut-down.

Substitution of parameters from the reader's experience will permit a comparison with de Heer's criterion for an adequately protected system - no more than 1% added risk as compared with that experienced in the general environment. For the 20- to 30-year-old worker with a yearly fatality rate of one per thousand, this would indicate an acceptable MTBE of 1×10^5 years.

REFERENCES

(1) de Heer, H.J.,Chemical Engineering, February 19, 1973, pp 121-128.

(2) Benjaminsen, J.M. and van Wiechen, P.H., IEEE Transactions on Industry and General Applications, Vol. IGA-5, No. 3, May June 1969, pp 242-249.

APPENDIX

In developing formulae for the probabilities of dangerous events (calamities) following from the failure of protective devices, de Heer (1) restricted his attention to devices having the same failure rate μ and the same average inoperative period τ_0 before repair. The following derivation is simpler than de Heer's and allows formulae to be found for cases where the parameters of the protective devices differ.

Let us assume that a protective device M_1 has a failure rate μ_1 and a mean inoperative period τ_{01}. The hazard H, against which M_1 operates, has a mean frequency of occurrence λ.

Referring to Figure 1, the system is put into normal operation at time zero. The probability that M_1 will fail at time τ_1 in the interval t to t + dt is

$$dP_1 = \mu_1 e^{-\mu_1 t} \, dt, \tag{1}$$

from de Heer's Equations 4 and 5.

The probability that H will occur at some time τ_H between t and $t + \tau_{01}$ (whether M_1 is operative or inoperative) is

$$F_H(\tau_{01}) = 1 - e^{-\lambda \tau_{01}}, \tag{2}$$

from de Heer's Equation 3.

The combined probability that H will occur at some time τ_H between t and $t + \tau_{01}$ after M_1 has become inoperative at τ_1 is

$$\begin{aligned} d P_{H,1} &= F_H(\tau_{01}) \, dP_1 \\ &= (1 - e^{-\lambda \tau_{01}}) \mu_1 e^{-\mu_1 t} \, dt. \end{aligned} \tag{3}$$

The total probability $P_{H,1}(T)$ of H occurring while M_1 is inoperative in some relatively long time interval from 0 to T is given by integrating Equation 3 i.e.,

$$\begin{aligned} P_{H,1}(T) &= \int_0^T (1 - e^{-\lambda \tau_{01}}) \mu_1 e^{-\mu_1 t} \, dt \\ &= (1 - e^{-\lambda \tau_{01}})(1 - e^{-\mu_1 T}) \end{aligned} \tag{4}$$

If we take the unit of time to be one year and set T = 1 in Equation 4 we obtain $P_{H,1}$ the average yearly rate of occurrence of dangerous events combining M_1 with H.

$$P_{H,1} = (1 - e^{-\lambda \tau_{01}})(1 - e^{-\mu_1}), \quad (5)$$

or $$P_{H,1} = \lambda \tau_{01} \mu_1 \text{ approximately,} \quad (6)$$

if $\lambda\tau_{01}$ and μ_1 are much smaller than 1. This is equivalent to de Heer's Equation 16.

In the applications discussed in the present paper, μ_1 is of the same order as 1, or greater, and Equation 6 is not valid. Equation 5 must be approximated by

$$P_{H,1} = \lambda \tau_{01} (1 - e^{-\mu_1}) \quad (7)$$

Now suppose that there is a second protective device M_2 having a failure rate μ_2 and a mean inoperative period τ_{02}, and that the dangerous event can only occur if M_2 and M_1 are both inoperative when the hazard H occurs.

Referring to Figure 2, the probability that M_2 will fail at time τ_2 in the interval t to t + dt is

$$dP_2 = \mu_2 e^{-\mu_2 t} dt. \quad (8)$$

The probability that a dangerous condition combining M_1 with H, represented by H,1 in Figure 2, will occur at some time τ_H between t and $t + \tau_{02}$ (whether M_2 is operative or inoperative) is

$$F_{H,1}(\tau_{02}) = 1 - e^{-P_{H,1}\tau_{02}} \quad (9)$$

The combined probability that the combination of circumstances represented by H,1 will occur at some time $\tau_{H,1}$ between t and $t + \tau_{02}$ after M_2 has become inoperative at τ_2 is

$$dP_{H,1,2} = F_{H,1}(\tau_{02})\, dP_2$$

$$= (1 - e^{-P_{H,1}\tau_{02}}) \mu_2 e^{-\mu_2 t} dt \quad (10)$$

The total probability $P_{H,1,2}(T)$ of H occurring while M_1 and M_2 are both inoperative in some relatively long time interval from 0 to T is given by integrating Equation 10, i.e.,

$$P_{H,1,2}(T) = \int_0^T (1 - e^{-P_{H,1}\tau_{02}}) \mu_2 e^{-\mu_2 t} dt$$

$$= (1 - e^{-P_{H,1}\tau_{02}})(1 - e^{-\mu_2 T}) \quad (11)$$

Setting T = 1 year as before we obtain $P_{H,1,2}$ the average yearly rate of occurrence of dangerous events combining M_2 and M_1 with H.

$$P_{H,1,2} = (1 - e^{-P_{H,1}\tau_{02}})(1 - e^{-\mu_2}) \quad (12)$$

or $P_{H,1,2} = P_{H,1}\tau_{02}\mu_2$, approximately, if $P_{H,1}\tau_{02}$ and μ_2 are much smaller than 1.

Inserting $P_{H,1}$ from Equation 6,

$$P_{H,1,2} = \lambda\mu_1\mu_2\tau_{01}\tau_{02}. \quad (13)$$

If we set

$$\tau_{01} = \tau_{02} = \tau_0$$

and $\mu_1 = \mu_2 = \mu$,
we obtain

$$P_{H,1,2} = \lambda\mu^2\tau^2,$$

which is equivalent to de Heer's Equation 28.

But when μ_2 is not small compared to 1, Equation 12 must be approximated by

$$P_{H,1,2} = P_{H,1}\tau_{02}(1 - e^{-\mu_2})$$

Inserting $P_{H,1}$ from Equation 7, $P_{H,1,2} = \lambda\tau_{01}\tau_{02}(1 - e^{-\mu_1})(1 - e^{-\mu_2})$ (14)

The extension of Equation 14 to greater numbers of protective devices is obvious. In the case of three protective devices the rate of occurrence of dangerous events involving the failure of all three protective devices and the occurrence of the hazard is

$$P_{H,1,2,3} = \lambda\tau_{01}\tau_{02}\tau_{03}(1 - e^{-\mu_1})(1 - e^{-\mu_2})(1 - e^{-\mu_3}) \quad (15)$$

In all cases the Mean Time Between Dangerous Events is given by the reciprocal of the rate of occurrence. i.e.,

$$MTBE_{H,1,2,3} = 1/\lambda\tau_{01}\tau_{02}\tau_{03}(1 - e^{-\mu_1})(1 - e^{-\mu_2})(1 - e^{-\mu_3}) \quad (16)$$

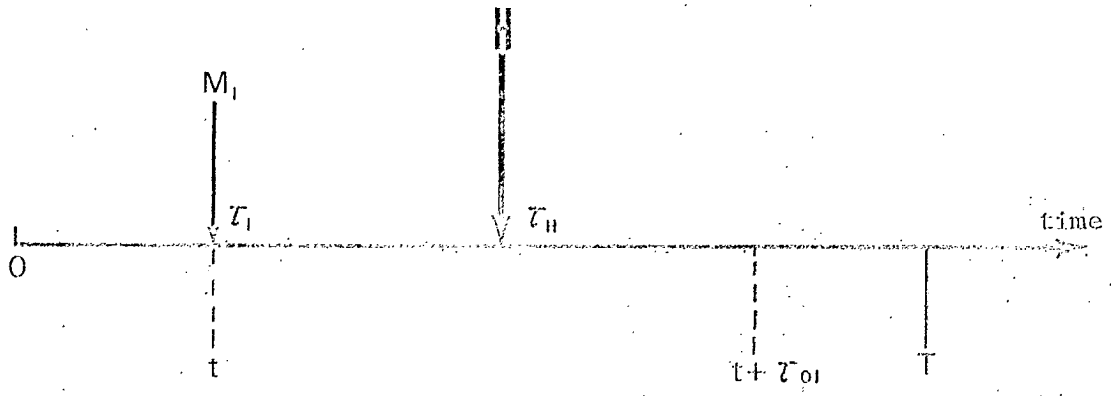

Figure 1 Time diagram of the occurrence of hazard while the protective device is inoperative.

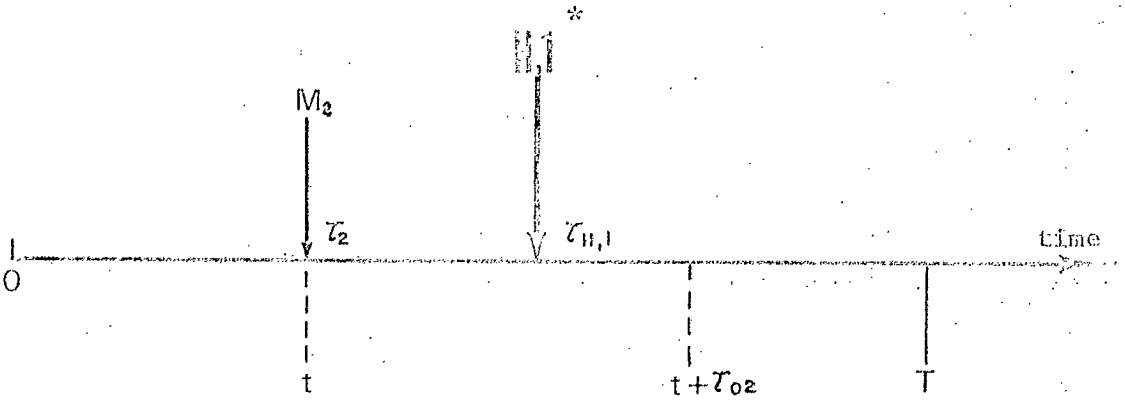

Figure 2 Time diagram of the occurrence of hazard while the first and second protective devices are inoperative.

* Where H,1 is a hazardous condition H which occurs during an open mode failure of protective device M_1 - i.e. the condition shown in Figure 1.