Economy-Based Countermeasure Decisions—Tutorial Guidance for System Safety Engineers

T-07-00400

August 2007

Prepared by:
Clark Kilgore
P.L. Clemens, P.E., CSP
A-P-T Research, Inc.
4950 Research Drive
Huntsville, AL 35805

Contents

Reference 1 (Stephenson)
Risk = "Risk—Mathematically, expected loss; the probability of an accident multiplied by the quantified consequence [severity] of the accident…"

$$R = S \times P^*$$

S = Severity

P = Probability

R = Risk

ABSTRACT

In bringing the risk of a hazard under control, the system safety practitioner is chiefly concerned with the availability of countermeasures and their effectiveness at controlling risk. While countermeasure cost is also of concern, decisions whether to adopt one or another of competing countermeasures are often based only on informally reckoned economic considerations. However, a more exact evaluation of the economic worth of adopting a given countermeasure can often be derived with relative ease if based on the fundamental mathematical definition of risk. Doing so helps to guide selection of a particular countermeasure, if any, from among competing ones. Practical examples readily support this proposition.

BACKGROUND

THE NATURE OF THE NEED

When a hazard is found which poses risk to a particular asset within a system, the level of risk is calculable. A countermeasure is proposed to reduce this risk to a lower level which is also calculable. The cost of adopting the countermeasure is known. The costs include implementing, maintaining, operating, and ultimately decommissioning the countermeasure in addition to initial outlay.

Practical questions now arise. Is there an economic advantage to be gained? Will the reduction in risk warrant the cost of adopting the countermeasure? Should a more effective or a less costly countermeasure be sought? Should several less costly options be implemented instead of a single expensive one? Should the status quo be maintained?

DEFINING RISK QUANTITATIVELY

To decide the merit of adopting a countermeasure, "before" and "after" levels of risk must be found. Many texts define risk as the simple mathematical product of the severity (S) of the harm the hazard may produce through a loss event and the probability (P) that the loss event will occur. Reference 1 is an example[2]. Thus risk (R) is given by this simple relationship.

[2] The definition for risk has long been accepted and has prestigious precedent far earlier than Reference 1—e.g., in 1711 Abraham de Moivre wrote, in De Mensura Sortis, "The risk… is the reverse of expectation; and the true measure of it is the product of the sum adventured [i.e., severity of potential loss] multiplied by the probability of the loss."

* Each author's own selection of symbols for the mathematical terms is used here, shown as they appear in the quotations taken from the references. There are no universally recognized symbols for these terms. Terms and symbols found in the text of this paper are those adopted for classroom use by the American Society of Safety Engineers.

$$R = S \times P \tag{1}$$

To assess risk quantitatively, it is necessary to express its severity and probability components quantitatively and carry out this multiplication. Numerical values must be assigned to the level of severity of the harm that may be caused by the hazard and to the level of probability that this harm will occur. Because probability is dimensionless, the dimensional units in which risk is expressed will be those conveyed by the severity term. Also because probability must apply to a specific interval of time, or to a particular operating cycle, trial, mission, or group of these, the value of risk that is found will apply only to that same interval, cycle, trial, mission, or group.

These concepts may be more readily grasped if they are expressed visually. Figure 1 presents a plot of Severity Value (the S term in Eq. 1) as a function of Loss Probability for various values of Risk. Logarithmic scales have been chosen for the axes here in order to encompass greater numerical spans than can be shown using linear scales. The diagonal lines that appear are isorisk contours, i.e. contours along which risk, the product of severity and probability, has a constant value. Thus the value of risk represented by point A, $(10^{-5} \times 10^{6}) = 10$, is equal to the risk value expressed by Point B, $(10^{-2} \times 10^{3}) = 10$. For the point shown as Q, risk is evaluated as the product of 3×10^{4} (the loss severity value) and 2×10^{-5} (the probability value), giving a risk value of 6×10^{-1}.

Reference 2 (Leveson)
Hazard Severity = “Hazard severity is defined as the worst possible accident that could result from the hazard…”

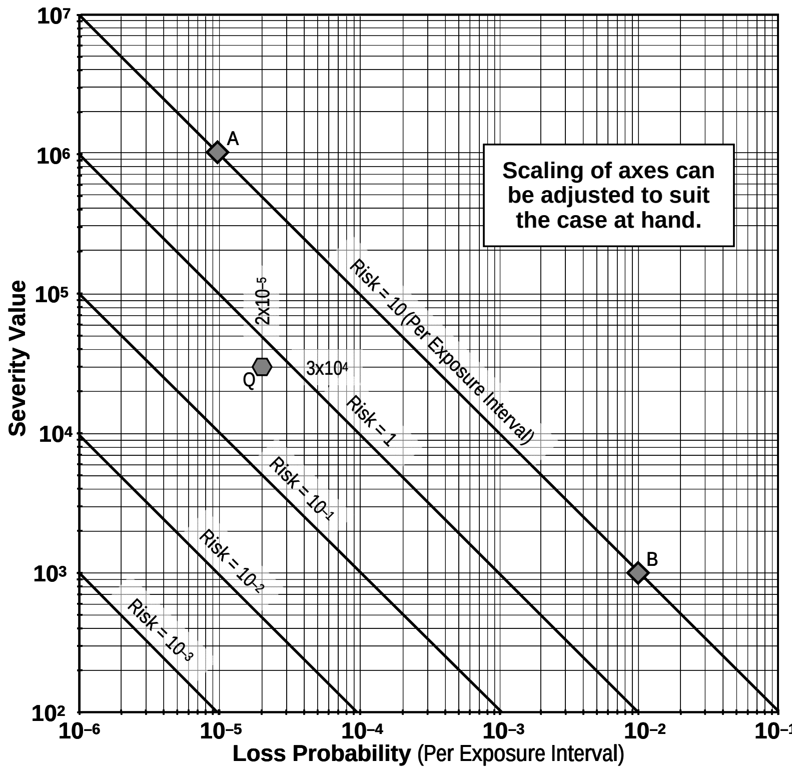

Figure 1 **Loss Values for Various Loss Probabilities**

EVALUATING SEVERITY

Of the two components of risk; severity and probability, severity is usually quantified with greater ease. In many cases, the cost of recovery from a posited loss event can be estimated and taken to represent severity. By convention in risk assessment, the severity component of risk for a hazard is often taken as the worst possible level of harm that may be produced by the hazard. Reference 2 presents this convention. This is also often called the worst credible level to distinguish it from the worst conceivable level, the latter being a level that can be imagined but is patently unreasonable to consider.

For many hazards, harmful outcomes will be more likely at lower levels of severity than the worst credible case. However, the products of multiplying these lower levels of severity and their accompanying increased probabilities will be more or less constant for an array of outcomes. They will therefore represent much the same value of risk. The practice of assessing risk for the worst credible outcome is further supported on the argument that the result will customarily be pessimistic. Exceptions to this generality arise and should be guarded against. Reference 3 deals with such exceptions.

Reference 4 Loss Rate (Browning)
"Loss Rate—…a valid loss exposure [a hazard] will present, for the loss event T, a characteristic loss rate R_T, equal to the severity multiplied by the frequency:

$R_T = S_T \times F$

The author gives these definitions for the terms in this expression:

R_T: Loss Rate, defined as quoted above

S_T: Loss Severity—"…the sum of all the costs attributable to one occurrence of the loss event T.

Loss Frequency—"…b will occur at a frequency set by the probability P_T [which is] a fraction, between 0 and 1, where 0 represents intrinsic impossibility and 1 represents absolute certainty."

Note: Here, F represents true frequency of occurrence rather than classical probability. Thus it is possible for the value of F to exceed unity. This would not be the case were it to represent probability, P_T, which is further defined by the author as "the mathematical likelihood of [a loss event] in a specified interval of time, or in the course of a particular operational cycle, or trial, or mission."

λ = Failure Rate

P_F = Failure probability of occurring in period T

EVALUATING PROBABILITY

The value of probability to be applied in assessing risk must represent the likelihood of experiencing a loss outcome at the same level of harm for which severity is evaluated, customarily the worst credible level. The probability value must apply to the specific duration for which risk is to be assessed. As it is put in Appendix Reference 4, probability is "the mathematical likelihood of [a loss event] in a specified interval of time, or in the course of a particular operational cycle, or trial, or mission." The value of risk that is assessed using this expression of probability then applies to that same specified interval of exposure and only to that interval.

Consider, for example, that risk is to be assessed for the hazard of experiencing the crash of a computer hard drive. Probability will be based on the characteristics of the equipment, service stresses, environmental stresses, and some specified number of operating hours. The hard drive crash risk that is evaluated will apply to this same number of operating hours. Severity in this case can be assumed to amount to the overall cost of replacing the hard drive. Some may wish, with good reason, to include the worth of lost data as a component of severity.

To evaluate probability, various approaches are available:

- Use of experience-based data for the same or similar phenomena.
- Use of published tables. These usually express failure rate (λ), from which failure probability (P_F) can be calculated. The relationship between the two is taken up in the following section. An appendix in Reference 5 presents an assortment of failure rate data sources.
- Estimation based on engineering judgement[3]. Reference 5 provides guidance for estimating failure probabilities.

DEALING WITH DIMENSIONAL DISTINCTIONS

Needs for quantitative risk assessments fall predominantly into two broad categories. Handling of the probability component of risk differs between one-time loss events and recurring loss events.

[3] Applying heuristic judgement in probabilistic risk assessment is inescapable. Judgement must be used, if only in the selecting of an analytical model.

MTTF = Mean Time To Failure

MTBF = Mean Time Between Failures

$\mathcal{R}$ = Reliability, the probability of no loss events over the interval T

ε = The Naperian base, 2.718+

T = Exposure Interval

ONE-TIME LOSS EVENTS

In one-time cases, there is need for knowing the probability of a loss event occurring at a particular level of severity during a specified period. The number of occurrences that might arise is not of interest. Either of two factors might lead to this need:

- Concern is for a high-severity potential outcome (i.e., an extreme perceived severity component of risk), or
- The nature of the hazard or of the hazard ensemble[4] precludes recurrences.

The probability of the crash of a specific aircraft while on a particular flight would be an example one-time event. Probability of destruction of a rare painting by fire, or the probability that an individual might succumb to a fatal disease during a selected decade of life are others. Irrecoverability or irreparability characterizes these cases.

The relationship between failure rate (λ) and Mean Time To Failure (MTTF) is important. Mean Time Between Failures (MTBF) will occupy the same role in the case of repeated loss events taken up later. From MTTF, failure rate (λ) is found (Reference 6):

$$\lambda = \frac{1}{MTTF} \qquad (2)$$

Notice that λ acquires the dimensions of *rate* or *frequency*—i.e., the reciprocal of units of time, of operational cycles, trials, missions, etc. This expression appears in the Poisson distribution[5] (Reference 6) for the limiting case of a stochastic system experiencing *no* loss event occurrences:

$$\mathcal{R} = \varepsilon^{-\lambda \mathrm{T}} \qquad (3)$$

Here, $\mathcal{R}$ = Reliability (the probability of no loss events over the interval T)

ε = The Naperian Base, 2.718+

λ = Failure Rate

[4] A hazard ensemble is a collection of hazards any of which can lead to a particular loss event.

[5] Many other, more sophisticated models than the Poisson exponential relationship are found in the literature. Their use is justified if a large body of failure data is available. Such databases are prevalent in work with large-scale production items, but are not often available in work with high technology developmental systems.

N = Total count of loss events occurring in period T

L_E = Expected Loss

T = Exposure Interval (period for which probability is to be evaluated; units are those used to express MTTF)

It follows that the probability of *some* (i.e., one or more) loss events (P_F) must be:

$$P_F = 1 - \mathcal{R} = 1 - \varepsilon^{-\lambda T} \quad (4)$$

It can be shown that if the exposure interval is brief compared to MTTF, then, as a useful approximation:

$$P_F = 1 - \varepsilon^{-\lambda T} \cong \lambda T \quad (5)$$

This approximation yields small errors—less than 11% for values of T less than 0.2 MTTF. The errors produce, in any case, only pessimistic results—i.e., values for P_F that are higher than those arrived at using the complete expression.

From Equation 1 and Equation 5, risk now becomes:

$$R = S(1 - \varepsilon^{-\lambda T}) \quad (6)$$

Using Equation 5, Equation 6 can now be approximated as:

$$R \cong S(\lambda T) \quad (7)$$

REPEATED LOSS EVENTS

In the second category are instances in which a hazard or hazard ensemble threatens to produce repeated loss events. The concern here is for cumulative risk over a specified period. A particular motor vehicle may suffer a number of flat tires over its lifetime of use, for example. It is then the likely accumulated total loss over a specified period during the duration of ownership that is of interest.

The total count (N) of loss events to be expected from a hazard over a specified period (T) must now be used rather than the probability of one or more events, as had been the case. And it is total expected loss (L_E) that is to be evaluated rather than classical risk. Thus, following from the form of Equation 1:

$$L_E = SN \quad (8)$$

Where[6] $N \cong \lambda T$

$$\text{Thus } L_E \cong S\lambda T \quad (9)$$

[6] This and many of the equations that follow are shown as approximations. They approximate the Poisson distribution model for cases in which T<MTTF. They are often called "rare event" approximations.

ΔR = Reduction in Risk

ΔL_E = Reduction in Loss

Evaluating Countermeasure Worth

The One-Time Loss Event

Consider that a particular hazard poses one-time risk at some level (R_1) and that a countermeasure is contemplated that will reduce this risk to a new level (R_2) by lowering either severity, probability, or both. Then the reduction in risk (ΔR) may be expressed as:

$$\Delta R = R_1 - R_2 = (S_1 P_{F1}) - (S_2 P_{F2}) \qquad (10)$$

Repeated Loss Events

With repeated loss events at issue, total expected loss (L_E) from Equation 9, replaces risk (R) in Equation 10. The result is:

$$\Delta L_E = L_{E1} - L_{E2} \cong [(S_1 \lambda_1) - (S_2 \lambda_2)]\ T \qquad (11)$$

ΔL_E is the reduction in loss.

Examples

A One-Time Loss Event – Transporting an Art Treasure

The Scenario

An insurer is asked to evaluate the risk of transporting an irreplaceable art treasure across the continent. These particulars apply:

- Value of item: $13M (This becomes the S term in Equation 6)
- Shipping cost: $2600
- Distance to be shipped: 2900 mi (This becomes the T term in Equation 6)

In shipments of this kind the threat of total loss of cargo through a highway accident is reckoned at ~ 3.3×10^{-8} per transport mile. This becomes λ in Equation 6.

Using Equation 6 to evaluate risk:

$$R = 13 \times 10^{6}(1 - \varepsilon^{-(3.3 \times 10^{-8})(2.9 \times 10^{3})}) = \$1244.00$$

This is the dollar value for the risk of loss of the art treasure as a consequence of a highway accident in the course of the trip.

To reduce risk, shipment by air is considered as a candidate countermeasure against the threat of loss of the art treasure. (Time in transit has been considered inconsequential, whether by truck or by air.) The shipping cost, however, is now $8400, an increase of $5800.

The probability of loss of cargo by this mode of transportation, based on the insurer's database, is ~ 1.2×10^{-8} per transport mile.

Again using Equation 6,

$$R = 13 \times 10^{6}(1 - \varepsilon^{-(1.2 \times 10^{-8})(2.9 \times 10^{3})}) = \$452.39$$

Air shipment as a countermeasure affords a risk reduction of:

$$\$1244.00 - \$452.39 = \$791.61$$

This is insufficient to offset the $5800 increase for air shipment. Shipment by truck remains the favoured transportation mode if economy is to be the sole determinant.

Much the same result would have been obtained by substituting the approximation offered as Equation 7 into Equation 10 and recognizing that $S_1 = S_2$, and $T_1 = T_2$:

$$\Delta R = R_1 - R_2 \cong ST(\lambda_1 - \lambda_2)$$

$$\Delta R \cong (13 \times 10^{6})(2.9 \times 10^{3})(3.3 \times 10^{-8} - 1.2 \times 10^{-8}) = \$791.70$$

Repeated Loss Events – A Rocket Propellant Blender

The Scenario

A facility manufacturing solid propellant rocket motors uses a group of blending machines to formulate and combine propellant and oxidizer materials before casting. A partially congealed mass of propellant material sometimes develops within a blender, a phenomenon called "clodding". Blender mixing vanes encounter these clods, causing them to break away from their supporting arms. The sundered vanes then become embedded in the propellant slurry. Recovery from a vane break is costly in interruption of production, cleanup man-hours, and equipment replacement. Cleanup activities can also expose personnel to the propellant material.

A torque-limiting coupling with a slip detector and an alarm feature is proposed as a countermeasure against the probability of vane breakage. The alarm prompts shutdown when a torque set point is exceeded. The clod can then be removed with a minimum of downtime and product loss.

Data shown in Table 1 characterize the performance of each blending machine in the group and indicate the anticipated outcome of adopting the countermeasure:

C_C = Countermeasure Cost

m = Countermeasure Maintenance Cost

i = Interest Rate Assumed

Benefit = Recognizable increase in production, income, status, etc. over current levels derived from countermeasure.

Cost = Monetary outlay to implement countermeasure

B-C = Benefit to Cost

Benefit-Cost Ratio Analysis = A formal discipline used to help assess the case for a project or proposal. The greater the benefit is in comparison to the cost, the more desirable the project. Units:unitless. > 1 is desired

Table 1. Blending Machine Performance

Current Vane Break Rate (Now) (experience-based)	0.008/production day	λ_1
Vane Replacement Cost (avg., incl. cleanup, product loss, and downtime)	$1,288.00	$S_1 = S_2$
Countermeasure Cost (Torque Limiter) (incl. installation)	$8,360.00/machine	C_C
Countermeasure maintenance cost	$205.00/year/machine	m
Anticipated Vane Break Rate (New) (est., with torque limiter)	0.003/production day	λ_2
Anticipated Operating Duration	8 years (2,000 production days)	T
Interest Rate Assumed	10% or 0.10	i

THE QUESTION

Would a reduction in expected loss warrant adopting the torque limiter as a countermeasure against the risk of vane breakage?

By performing a basic Benefit-Cost (B-C) ratio analysis on the proposed countermeasure and comparing it to the status quo, a degree of desirability can be determined. Given management is of the mindset to make changes, and they have the needed capital to implement them, the option that presents the greatest B-C ratio is deemed the appropriate choice. Should the benefit derived be small, management may opt to wait or look at others areas for investing the available funds. In the example above, we assume that the process in question will produce a certain benefit regardless of the number of vanes broken. By reducing the probability of breaking a vane, an added benefit can be achieved. Therefore in the calculations below, we will only examine the cost factor associated with each option. The option that results in the lowest cost would yield the largest B-C ratio holding the benefit equal for each option. An annual maintenance cost will be incurred for both options (either implementing countermeasure or remaining with status quo). This cost is $205.00 each year and is denoted by the variable m. In order to account for the monetary expenditures accurately, we must assume an interest rate. For this example we chose 10%. Since there are no specific benefits defined in the problem, we assume that both options under consideration yield the same benefit. Therefore, a comparison of the costs

PV = Present Value is the value of money discounted to account for the time value of money and other factors such as investment risk. Present value of money is always less than the corresponding future value. This type of calculation is often used when comparing cash flows of like items. Units: dollars

Reference 7 (Abol)
Analysis = Vane breakage/year
= (0.008)(2,000 days)

= 16 vanes/8 years

Lifecycle = 2,000 days or 8 years = 2 vanes/year

Cost of vane replacement = $1,288/vane

Cost/year = (1288/vane)(2 vane/year) = $2,576/year+205 = $2,781/year

Maintenance cost/year = 205/year

Using a Present Value equation to determine the present value of costs

$$PVc = C\frac{(1+c)^n - 1}{i(1+i)^n}$$

$$PVc = 2781\left(\frac{(1+c)^n - 1}{i(1+i)^n}\right)$$

$$PVc = 2781\left(\frac{(1.1)^8 - 1}{0.1(1.1)^8}\right)$$

$$PVc = 2781\left(\frac{1.1435}{0.21435}\right)$$

$$PVc = 2781(5.335)$$

$$PVc = \$14{,}836.635$$

$$PVc = \$14{,}836.64$$

associated with each option is used as the deciding factor. Any reduction in cost would be considered an increase in the benefit of the operation.

OPTION 1: STATUS QUO

Rate of vane breakage = 0.008/production day

Life of operation = 2,000 days

Expected number of vanes broken over life of operation = (0.008 vanes/production day)(2,000 production days) = 16 vanes

Cost to replace a broken vane = $1,288.00/vane

Cost of replacing broken vanes over the life of operations = (16 expected vanes broken)($1,288.00/vane to replace) = $20,608.00

Maintenance cost over life of operation = (8 years)($205.00/year) = $1,640.00

Total annual cost for Option 1, C_1 = Cost of replacement per year + annual maintenance costs

=>$20,608/8 + $205.00 = $2,781.00

Using a Present Value (PV) calculation at time 0 to determine the present value of the annual costs, the true value of dollars spent can be determined.

$PV = (1+i)^n – 1/i(1+i)^n$

$PV = (1+0.1)^8 – 1/0.1(1+0.1)^8 = 5.33$

Now, using the annual cost of $2,781.00 and the PV factor of 5.33, the present value of the cost adjusted for interest is:

5.33($2,781.00) = $14,822.73

OPTION 2: IMPLEMENT THE COUNTERMEASURE

Cost of countermeasure = $8,360.00

Rate of vane breakage = 0.003/production day

Life of operation = 2,000 days

Expected number of vanes broken over life of operation = (0.003 vanes/production day)(2,000 production days) = 6 vanes

Cost of vane replacement = $1,288.00/vane

Cost of replacing broken vanes over the life of operations = (6 expected vanes broken)($1,288.00/vane to replace) = $7,728.00

Net Annual Savings = Benefit derived by subtracting the annual cost of countermeasure options from annual cost of status quo.

Maintenance cost over life of operation = (8 years)($205.00/year) = $1,640.00

Total annual cost for Option 2, C_2 = Cost of replacement per year + annual maintenance costs

=>$7,728/8 + $205.00 = $1,171.00

Again, using the PV factor derived above with the new annual cost, a new present value is determined.

= 5.33($1,171.00) = $6,241.43

Combining the initial cost of the countermeasure with the adjusted annual cost, the true cost of the countermeasure is:

$8,360.00 + $6,241.43 = $14,602.43

Net annual savings is ($2,781.00 - $1,171.00) = $1,610.00

OPTION 1: STATUS QUO

Cost = $14,822.73 over life cycle

OPTION 2: COUNTERMEASURE

Cost = $14,602.43 over life cycle

PAYBACK PERIOD DETERMINATION

The payback period—i.e., the duration of operation over which the saving in cost owing to the reduction in risk exactly equals the cost of adopting the countermeasure can be found by determining how many years of saving $1,610.00 it will take to equal the total cost of implementing the countermeasure.

Total cost = $14, 602.43

Payback = $14,602.43/$1,610.00 = 9.07 years

CONCLUSION

Though the countermeasure does reduce the replacement cost of a broken vane by ($2,781.00-$1,171.00) = $1610.00/year, the initial cost of implementing ($8,360.00) makes this option undesirable. Also, the Payback period exceeds the expected life of operation for process. If the cost of the countermeasure was to be reduced, or an increase in benefit was achieved, the countermeasure should be re-evaluated.

CONCLUDING REMARKS

Too often, selecting a countermeasure for the control of risk is based on intuitive perception rather than applying risk management principles found in the practice of system safety. In many cases, applying those principles is not at all a complicated process. A rational selection from among competing countermeasures can be based simply on the basis of the relative cost and effectiveness of the feasible candidates. As a simple test of effectiveness, the cost of adopting a countermeasure should be offset by the reduction in risk that is realized. The residual risk that remains after adopting the countermeasure must be acceptably low. Applicable codes and standards must be satisfied, of course. Beyond that, accepting residual risk is a prerogative reserved to management.

When matters of life, limb, and health are at risk, the process becomes more complex and falls beyond the scope of the treatment intended here.

THE AUTHORS

Clark Kilgore is a Senior Safety Engineer with APT Research, Inc. He has worked in both the System and Flight Test Safety areas for the Department of Defence's Ground-based Interceptor Program and is currently supporting System and Flight Test Safety efforts for the next generation of interceptors. He resides in Madison, AL.

Pat Clemens performs system safety engineering work for APT Research, Inc. He is a past president of the Board of Certified Safety Professionals. He has developed and implemented many system safety programs in both government contracting and in the private sector. He teaches system safety-related courses for various private corporations, for NASA, and on university campuses. He makes his home in Tullahoma, Tennessee.

REFERENCES

1. Stephenson, Joe; "System Safety 2000: A Practical Guide for Planning, Managing, and Conducting System Safety Programs"; Van Nostrand Reinhold; 1991; ISBN 0-442-23840-1
2. Leveson, Nancy; "Safeware: System Safety and Computers"; Addison-Wesley; 1995; ISBN 0-201-11972-2
3. Clemens, P. L.; "Worst Credible Event—An Important but Flawed Convention"; Journal of the System Safety Society; Vol. 35, No. 2.
4. Browning, R. L.; "The Loss Rate Concept in Safety Engineering"; Marcel Dekker; 1980; ISBN 0-8247-1249-8
5. Ebey, S. F. and P. L. Clemens; "Making and Adjusting Failure Probability Estimates Using a Bayesian Approach"; paper presented at the 14th International Conference of the System Safety Society (Proceedings published); 1966
6. Raheja, Dev G.; "Assurance Technologies, Principles and Practices"; McGraw-Hill; 1991; ISBN 0-07-051212-4
7. Abol Ardalan, D. SC.; "Economic and Financial Analysis for Engineering and Project Management"; Technomic Publishing; 2000