Safety, Reliability and Risk Analysis: Beyond the Horizon – Steenbergen et al. (Eds)
© 2014 Taylor & Francis Group, London, ISBN 978-1-138-00123-7

Multi layer safety: A generally efficient solution or work for all

J.K. Vrijling
Technical University of Delft, Delft, The Netherlands

ABSTRACT: The application of the "safety chain" consisting of proaction, prevention, preparation, repression/mitigation, recovery and learning will be studied in this paper. The chain appears to be a multi layer system, that is at least as safe as the safest layer. It will additionally be observed that the effectiveness of resources spent in prevention is most probably higher than on repression, because repression becomes only effective after the disaster has occurred and at least the economic damage has become a fact. Several examples of multi layer safety systems will be analysed in this paper. Mathematical methods of risk analysis and probabilistic reasoning are essential in the design and the understanding modern safety systems. Verbal reasoning alone is insufficient.

1 INTRODUCTION

Since 2008 Dutch risk managers advocate the application of the "safety chain" consisting of proaction, prevention, preparation, repression/mitigation, recovery and learning. Proaction means to avoid the danger at all e.g. by not building a city in the Mississippi delta or on top of a tectonic faultline. Prevention indicates the construction of structures that can withstand the force of the rare threat and protect people and goods. Preparation points to planning rescue and mitigation activities in advance. Repression addresses the actual rescue activities after the disaster has struck. Building waterproof facilities or houses on piles or mounds that will be damaged less in case of inundation is indicated by mitigation. Also insuring the properties against the consequences of an inundation falls in this category. Finally the damage should be repaired and the society should be put on its feet again. This is the recovery phase of risk management.

The risk management experts state that all links of the safety chain have to be addressed by the responsible authorities. This is based on the reasoning that a chain cannot function if an element is omitted. Closer inspection of the safety chain however reveals that it is a parallel system of multiple layers, that is at least as safe as the safest layer. Additionally it should be noted, that that the effectiveness of resources spent in prevention is most probably higher than on repression, because repression becomes only effective after the disaster has occurred and the economic damage is a fact. New Orleans has shown that people and movable property can be saved, but fixed property is subjected to the force of the flood and all economic processes are halted. If the evacuation and recovery expenditure would have been directed at the improvement of the defences, the disaster might have been avoided.

A similar but slightly different question arises in the siting and construction of hazardous installations. This treated more from the perspective of spatial planning and for some reason the consequences of a disaster are limited to human casualties in the area around the facility. Economic damage is neglected. The regulations stipulate that a risk analysis is made and shows that the individual risk is limited to 10^{-6} per year and that the group risk indicated by the FN-curve is below an advisory line. Permission is in principle granted if these conditions are fulfilled. However the local emergency services also contribute to the decision. They advise small changes in infrastructure that will facilitate rescue operations. In this process however they tend to consider the 10^{-6} scenario from the risk analysis and reach the conclusion that such an event will overpower their rescue capacity unless it is enhanced.

The central question is how expenditure should be divided over the various layers. Is it economically optimal to share the total expenditure between the layers in some proportion or would efficiency require that all money is spent on the layer that provides the highest marginal safety.

The economically acceptable probability of failure. One of the tasks of human civilizations is to protect individual members and groups to a certain extent against natural and man-made hazards. The extent of the protection was historically mostly decided after the occurrence of the hazard had shown the consequences. The modern approach aims to give protection when the risks are felt to be high. Risk is defined as the probability of a disaster i.e. a flood related to the consequences. As long as the modern approach is not firmly embedded in society, the idea of acceptable risk may, just as in the old days, be quite suddenly influenced by a single spectacular accident.

The estimation of the consequences of a flood or an industrial accident constitutes a central element in the modern approach. Most probably society will look to the **total** damage caused by the occurrence of a disaster (Vrijling[12]). This comprises a number of casualties, material and economic damage as well as the loss of or harm to immaterial values like works of art and amenity. Also the loss of trust in the technical system is a serious, but difficult to gauge effect as Tsjernobil and Fukushima have shown. However for practical reasons the notion of risk in a societal context is often reduced to the total number of casualties using a definition as: "the relation between frequency and the number of people suffering from a specified level of harm in a given population from the realization of specified hazards". If the specified level of harm is limited to loss of life, the societal risk may be modeled by the frequency of exceedance curve of the number of deaths, the FN-curve.[12]

The consequence part of a risk can also be limited to the material damage expressed in monetary terms as the Dutch Delta Committee did in 1960. It should be noted however, that the reduction of the consequences of an accident to the number of casualties or the economic damage may not adequately model the public's perception of the potential loss. The schematisation clarifies the reasoning at the cost of accuracy of the decision based on it.

The problem of the acceptable level of risk can be elegantly formulated as an economic decision problem. The expenditure I for a safer system is equated with the gain made by the decreasing present value of the risk. The optimal level of safety indicated by P_f corresponds to the point of minimal cost.

$$\min(TC) = \min(I(P_f) + PV(P_f \cdot D))$$

where:

TC = total cost
PV = present value operator
D = total damage given failure.

If despite ethical objections, the value of a human life is rated at V according to,[11] the amount of damage is increased to:

$$P_{d|fi} \cdot N_i \cdot V + D$$

where

N_i = number of inhabitants in polder *i*.
$P_{d|fi}$ = probability of drowning given failure.

This extension makes the damage an increasing function of the expected number of deaths. The valuation of human life is chosen as the present value of the nett national product per inhabitant. The advantage of taking the possible loss of lives into account in economic terms is that the safety measures are affordable in the context of the national income (see also Vrijling and Van Gelder[11]).

Omitting the value of human life, the decision problem as formulated by the Delta Committee[7,8] is given below. The investment I(h) in the protective dike system is given as a function of the crest level h by:

$$I(h) = I_0 + I_1(h - h_0)$$

where

I_0 = initial cost
I_1 = marginal cost
h_0 = existing dike level.

The annual probability of exceedance of the crest level of the dike is given by the exponential distribution of the storm surge level:

$$1 - F(h) = e^{-\frac{h-A}{B}}$$

The risk of inundation is equal to the probability of exceedance of the dike crest times the damage D in case of inundation.

$$Risk = e^{-\frac{(h-A)}{B}} \cdot D$$

Because the risk occurs every year the present value of the risk over an infinite period has to be taken into account

$$PV(Risk) = \sum_{i=1}^{\infty} e^{-\frac{(h-A)}{B}} \frac{D}{(1+r)^i} = e^{-\frac{(h-A)}{B}} \frac{D}{r}$$

where r = discount rate.

The total cost is the sum of the investment and the present value of the remaining risk that is accepted;

$$TC(h) = I_0 + I_1(h - h_0) + e^{-\frac{(h-A)}{B}} \frac{D}{r}$$

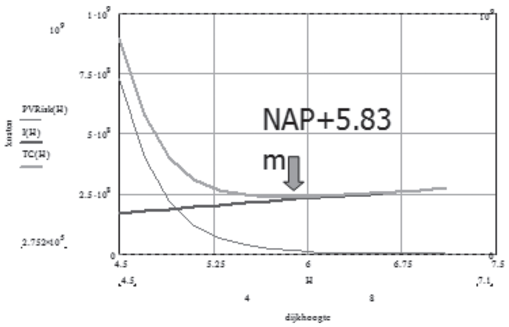

Figure 1. The economically optimal crest level.

Differentiating the total cost with respect to the decision variable h and equating the derivative to 0 gives an elegant result

$$\frac{\partial TC(h)}{\partial h} = I_1 - \frac{1}{B} e^{-\frac{(h-A)}{B}} \frac{D}{r} = 0$$

$$p_{f-h\,optimal} = e^{-\frac{(h-A)}{B}} = \frac{I_1 B r}{D}$$

The last expression shows that the acceptable probability increases with the marginal cost of dike construction, with the standard deviation of the storm surge level B and the rate of interest. It decreases with the damage that will occur in case of an inundation.

The Delta Committee[7,8] calculated an acceptable probability of inundation for Central Holland in 1960 of $8 \cdot 10^{-6}$ per year (Fig. 1). Some approximating calculations performed by Dutch engineers[14] in 2006 indicated an optimal level of $2 \cdot 10^{-4}$ per year for New Orleans. The present system that is built after Katrina has the planned safety level of 1/100 per year.

The economic criterion presented above should be one of the elements of the "technical" advice to the political decision process beside the individual risk and the group risk. All information of the risk assessment should be available in the political process.

2 AN EXTRA LAYER; INSURANCE

Insurance is one method of repressing the economic damage caused by an uncertain event. The insured pays an insurance premium every year and the insurer is obliged to refund the main part of the damage if the uncertain event occurs. The insurance premium will be at least equal to the expected value of the loss, the risk. However the insurer must add an allowance for transaction costs, risk aversion and profit. So generally the insurance premium is a factor g higher than the risk. This is especially true if the insured risks are fully dependent, because then all insured are hit simultaneously. This is the case in flood insurance contrary to commonly marketed insurance policies.

The model presented above is easily adapted for the case of insurance. Let us assume for the sake of simplicity that the insurer covers all damage *D* in return for a premium that is g times the risk.

$$Premium = e^{-\frac{(h-A)}{B}} \cdot g \cdot D$$

Now the total cost of prevention and insurance becomes

$$TC(h) = I_0 + I_1(h - h_0) + e^{-\frac{(h-A)}{B}} \cdot \frac{g \cdot D}{r}$$

Applying the same algebra as above the optimal probability of inundation is reduced by a factor *g* and becomes:

$$p_{f-optimal} = e^{-\frac{(h-A)}{B}} = \frac{I_1 B r}{g \cdot D}$$

The conclusion is that the safety of the flood defense should be increased by a factor g and the defenses increased in strength if the damage is privately insured. So for a country like the Netherlands, where a flood will doubtlessly mean a national disaster, that obliges the government of the stricken people to help to repair their properties and the infrastructure. The expenditure can be internationally borrowed. An insurance leads to increased cost without clear advantages. If the stricken area is however a small part of a large country, that might be left to it's own devices in recovery, a flood insurance might be wise. Especially if the country's policies lean more towards individual responsibility than state intervention. (In this analysis the failure of the insurer was excluded)

3 A TWO LAYER SYSTEM

Suppose a two layer system, where the layers are independent and the probability of failure of each layer *i* equals p_i. The risk becomes

$$Risk = p_1 \cdot p_2 \cdot D$$

The total cost of investment and the present value of the risk equals

$$TC(p_1, p_2) = I_0 - I_1 \ln(p_1) - I_2 \ln(p_2) + p_1 \cdot p_2 \cdot \frac{D}{r}$$

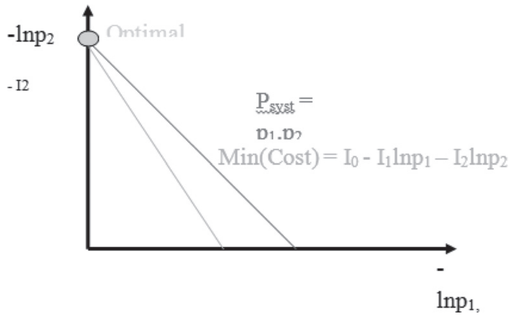

Figure 2. The economical optimization of a two layer system.

Differentiation with respect to p_i leads to a slightly more complicated result because the minimum lies at the border:

$$p_{f-optimal} = \min\left\{\frac{I_1 r}{D}, \frac{I_2 r}{D}\right\}$$

According to this simple model only the layer with the lowest marginal cost is applied, the other is omitted as shown in Fig. 2.

In this simple example the opinion of the risk management experts that all elements of the safety chain must be applied is again refuted. Such an example is of course no proof, but it is an indication that the safety chain or multi layer model in the simple interpretation gives no reliable guidance.

4 MULTI LAYER FLOOD SAFETY; DIKE AND PILES

One of the obvious short comings of the previous model is the independency of the layers. Generally the same hazard is threatening both layers. The first model is easy to expand by introducing an extra layer by elevating the houses, which shelter the people that live of the land, on piles of length l. The dike protects the value of the produce on the land. If the dike is overtopped the loss will equal D. If the flood level exceeds the length of the piles the n inhabitants of the house, each valued at V will drown.

The investment I(h,l) in the protective dike/pile system is given as a function of the crest level h and the pile length l by:

$$I(h,l) = I_0 + I_1(h) + I_2(l)$$

where I_0 = initial cost
I_2 = marginal cost of piles

The annual probability of exceedance of the crest level of the dike and the pile length is given by the same exponential distribution.

The risk of inundation equals the sum of the probability of exceedance of the dike crest times the damage D in case of inundation and the probability of exceedance of the pile length times the economic value of the loss of life n.V.

$$Risk = e^{-\frac{(h-A)}{B}} \cdot D + e^{-\frac{(l-A)}{B}} \cdot n \cdot V$$

Because the risk occurs every year the present value of the risk over an infinite period has to be taken into account

$$PV(Risk) = e^{-\frac{(h-A)}{B}} \frac{D}{r} + e^{-\frac{(l-A)}{B}} \frac{n \cdot V}{r}$$

The total cost is the sum of the investment and the present value of the remaining risk that is accepted;

$$TC(h,l) = I_0 + I_1(h) + I_2(l) + e^{-\frac{(h-A)}{B}} \frac{D}{r} + e^{-\frac{(l-A)}{B}} \frac{n \cdot V}{r}$$

Differentiating the total cost with respect to the decision variables h and l and equating the derivatives to 0 gives two separate results:

$$\frac{\partial TC(h,l)}{\partial h} = I_1 - \frac{1}{B} e^{-\frac{(h-A)}{B}} \frac{D}{r} = 0$$

$$\frac{\partial TC(h,l)}{\partial l} = I_1 - \frac{1}{B} e^{-\frac{(l-A)}{B}} \frac{n \cdot V}{r} = 0$$

leading to:

$$p_{f-h\ optimal} = e^{-\frac{(h-A)}{B}} = \frac{I_1 Br}{D}$$

$$p_{f-l\ optimal} = e^{-\frac{(l-A)}{B}} = \frac{I_2 Br}{n \cdot V}$$

The two expressions are similar. However it only makes sense to invest in dikes and piles, if the acceptable probability of exceedance of piles is smaller than that of the dike. A two layer system of dikes and piles is only warranted if

$$\frac{I_2 Br}{n \cdot V} \leq \frac{I_1 Br}{D} \text{ or simpler } \frac{I_2}{n \cdot V} \leq \frac{I_1}{D}$$

So simply speaking (assuming $I_1 \sim I_2$) if the value of the people is much larger than the damage to the land a two layer system is optimal. However according to economic theory there must be a relation between the value of the population and the value of the produce of their land.

Moreover the choice is in fact between a two layer system and a single layer dike system. In the last case the dike protects the people as well as the land and the safety should be increased to:

$$p_{f-h\ optimal} = e^{-\frac{(h-A)}{B}} = \frac{I_1 Br}{D + n \cdot V}$$

This means that a two layer system is only economically advisable if

$$\frac{I_2}{n \cdot V} \leq \frac{I_1}{D + n \cdot V}$$

thus the marginal cost of piles should be much smaller than dikes.

This crude example shows that the design of multi layer systems is far from simple. In many cases a single layer system will be most efficient. In the simple example treated above it is worthwhile to protect low value land with a small dike and to safeguard the accumulated value in the house and its inhabitants by elevating it on piles or a mound. To generalise these conclusions more cases have to be studied as well as the economic relation between the damage variables (here D,n,V). But it seems clear that a general policy that requires multi layered safety as a standard needs better analysis.

5 MULTI LAYER SAFETY; EMERGENCY SERVICES

It was already stated that an assumption behind multi layer safety seems to be that every layer can withstand the full force of the hazard. For the third layer, the emergency and rescue services this seems doubtful. In many real disasters the effectiveness of the emergency operations appeared to be limited. The Mont Blanc tunnel fire and the collaps of the Twin Towers, where courageous rescue workers lost their lives were already mentioned. In the Netherlands a exercise "Taskforce Management Flooding" (TMO) showed also that it is very unlikely that all people can be evacuated from the Central-Holland polder in case of a major storm surge. Only the consequences of a river flood that gives due advance warning, that it may exceed the crest level of the dikes, during its passage through Germany, can be mitigated by evacuation. If however the flood level is predicted not exceed the crest level, but the dike fails suddenly due to insufficient strength the rescue operations will start too late and their success has to be doubted. The same could be said for fire fighters that are expected to combat e.g. a BLEVE.

This poses the question which capacity of the rescue has to be laid out on these extreme scenario's, that seem to be implicitly chosen in planning the response. As an example the first model of the optimal dike crest is applied to the emergency operation. As a first step the FN-curves of all installations in an region are aggregated. This is the probability of exceedance line of the number of casualties in the region. It should be transformed into the FN-curve of the number of wounded. In a first approximation a multiplication by a factor of 10 (wounded/casualties) seems acceptable. Secondly the effectiveness of a rescue worker should be estimated. Here it is assumed that one worker brings c people back to health and safety. In order to find the economical optimal frequency the cost of the rescue worker per year w and the value of a human life V have to be introduced. The costs and the benefits even out if the rescue capacity is laid out at an accident with a probability of exceedance of:

$$p_{f-rescue\ optimal} = \frac{w}{c \cdot V}$$

So if the cost of labour is of the order of 10^5 €/y and the value of a live 10^6 € the design frequency varies between 1/10 to 1/(c.10) per year depending on the number of wounded saved. This differs by orders of magnitude from the probabilities of the extreme scenario's that are currently taken from the spatial planning related risk analyses to calculate the individual and group risk, as the basis for the planning of emergency operations.

6 CONCLUSIONS

The mathematical risk approach has great advantages compared with the present intuitive.

The classical approach was sketched to define the economical optimal level of risk. This was indicated as the acceptable risk. The decision on the level of acceptable risk is a cost/benefit judgement, that must be made from societal point of view. This mathematical optimum should be adopted as a basis for the "technical" advice to the political decision process. However all information of the risk assessment should be available in the political process. A decision that is political in nature, must be made democratically, because many differing values have to be weighed. The economic optimisation shows however that a fundamental reassessment of the acceptability of the risks is justified if the economic activities in the protected areas have grown or the relative importance has changed.

The application of the “safety chain” consisting of proaction, prevention, preparation, repression/ mitigation, recovery and learning was explained and analysed in some depth. The chain appears to be a multi layer system, that is at least as safe as the safest layer. It was additionally observed that effectiveness of resources spent in prevention is most probably higher than on repression, because repression becomes only effective after the disaster has occurred and at least the economic damage is a fact.

As a first example of multi layer safety flood insurance was analysed. It appeared that insurance forces to a higher level of protection because the insurance premium exceeds the risk by some factor. The total cost of prevention and private insurance will increase compared to prevention only. So in countries like the Netherlands where a flood will be a national disaster, insuring flood damage seems ill advised. A small community that cannot count on national aid in case of a disaster might however be wise to opt for insurance.

Thirdly a parallel system of two independent layers was economically optimized under the assumption that any level of safety could be reached at a cost that is a linear function of the logarithm of the failure probability. It appeared that the optimal investment was limited to one layer of protection, the layer with the lower marginal cost. This refutes in some sense the quick conclusion of the simple safety chain reasoning that every element should be addressed.

In the fourth place a safety system consisting of a dike and a house elevated on piles was economically analysed. The analysis resulted in two optimal design frequencies one for the dike crest and another for the elevation of the house. Only if the design frequency for the dike exceeds that of the piles a two layer system is economically efficient. This is the case if simply said the damage to the produce of the land is smaller than the value of the house and its inhabitants. As soon as the value of the damage to the land is considerably higher than that of the inhabited house the optimal system reduces to a dike only.

Although it is not permissible to draw general conclusions from examples, it is clear that a safety policy that recommends multi layer safety in all cases defies economic reasoning. It seems that in quite some cases single layer safety is economically optimal, although in a few cases multi layer safety proves to be more efficient.

Finally it is explained that multi layer safety assumes that each layer can withstand the hazard. The last layer, the emergency service, is certainly not able to deflect the full force of the small probability hazards. If this fact is neglected and the optimal design frequency of the emergency service is derived on a cost/benefit basis, the result is in the order of 1/10 per year i.e. much higher than 10^{-6} scenario’s used in chemical hazard studies or the 10^{-4} design storms applied in Dutch dike design. This means that the emergency services should concentrate on the suppression of incipient failure instead of the full accident. This is the old tradition of the “dike army” that limits itself to repairing incipient damage to the dike during storm surges. It lacks completely the resources to evacuate a polder on short notice.

It is clear from the examples in this paper that the mathematical methods of risk analysis and probabilistic reasoning are great aids in the design and the understanding modern safety systems. Verbal reasoning alone is insufficient.

REFERENCES

[1] Blockley, David, (1992): Engineering safety, London: McGraw-Hill*, ISBN 0-07-707593-5.*

[2] Guedes Soares, C. (2001): Dealing with strength degradation in structural reliability. In Risk-Based Design of Civil Structures, pp. 31–49, Eds. Pieter van Gelder, Alex Roos, Han Vrijling, Communications on hydraulic and geotechnical engineering, ISSN 0169-6548*, Report No. 01-1.*

[3] Hohenbichler, M., Rackwitz, R., (1983): First-order concepts in system reliability. *Structural Safety,* Vol. 1, p. 177.

[4] Nowak, A.S., Collins, K.R. (2000): Reliability of structures*, McGraw-Hill, ISBN 0-07-048163-6.*

[5] Stewart, Mark, G., Melchers, Robert, E. (1997): Probabilistic risk assessment of engineering systems, London: *Chapman and Hall, ISBN 0-412-80570-7.*

[6] Technical Advisory Committee on Water Retaining Structures (1989): Probabilistic design of sea defences, *CUR, Gouda.*

[7] van Dantzig, D, Kriens, J. (1960): The economic decision problem of safeguarding the Netherlands against floods. *Report of Delta Committee, Part 3, Section II.2 (in Dutch), The Hague.*

[8] van Dantzig, D, (1956): Economic Decision Problems for Flood Prevention, *Econometrica 24*, pp. 276–287, *New Haven.*

[9] Van Gelder, P.H.A.J.M., (1999): Statistical methods for the risk-based design of civil structures/ by Petrus Hermanus Antonius Johannes Maria van Gelder, Publisher S.l.: S.n., 1999, *ISBN 90-9013452-2*, p. 249.

[10] Vrijling, J.K. (2001): Review of dealing with strength degradation in structural reliability, In Risk-Based Design of Civil Structures, pp. 51–53, Eds. Pieter van Gelder, Alex Roos, Han Vrijling, Communications on hydraulic and geotechnical engineering, ISSN 0169-6548*, Report No. 01-1.*

[11] Vrijling, J.K. van Gelder, P.H.A.J.M., (2000): An Analysis of the Valuation of a Human Life, ESREL 2000 AND SRA—Europe Annual Conference, "Foresight and Precaution", vol. 1, pp. 197–200, Eds. M.P. Cottam, D.W. Harvey, R.P. Pape, & J. Tait, *May 14-17 2000 Edinburgh, Scotland, UK.*

[12] Vrijling, J.K., van Hengel, W., Houben, R.J., (1998): Acceptable risk as a basis for design, *RELIAB ENG SYST SAFE 59: (1) 141-150 JAN 1998* and Response to comments by J. Ramsberg on the paper "Acceptable risk as a basis for design", *RELIAB ENG SYST SAFE 67: (2) 211-212 FEB 2000.*

[13] ASCE, The New Orleans Hurricane protection System, What went wrong and why, ISBN 13-978-0-7844-0893-3, ASCE 2007.

[14] NWP, a Dutch perspective, Delft, 2007.